IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE SOLARWINDS CORPORATION SECURITIES LITIGATION	Case No. 1:21-cv-00138-RP CLASS ACTION JURY TRIAL DEMANDED

LEAD PLAINTIFF'S OMNIBUS MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

CASES

OTHER AUTHORITIES

I. INTRODUCTION

This case concerns SolarWinds' well-documented misstatements and omissions about its cybersecurity controls.[1] SolarWinds rose to prominence in the IT sphere by winning lucrative contracts with government agencies. To secure those contracts, SolarWinds held itself out to customers and investors alike as a cybersecurity stalwart. Its Vice President of Security Architecture, Defendant Tim Brown, published articles and spoke at length during interviews about the concrete efforts that SolarWinds supposedly took to keep sensitive client data secure. The Company set up a "Security Center" page on its website that featured a picture and video of Defendant Brown and an accompanying written "Security Statement"—a veritable manifesto on the Company's commitment to cybersecurity. In the Security Statement, Defendant Brown and SolarWinds made specific and detailed representations about the cybersecurity measures they supposedly had in place, including a dedicated security team, a stringent password policy, cybersecurity training for employees, and more.

In reality, SolarWinds bore no resemblance to the Company publicly described by Defendant Brown and the Security Statement. SolarWinds had no security team, no password policy, and no cybersecurity training. In 2017, SolarWinds' Global Cybersecurity Strategist Ian Thornton-Trump recognized the severely deficient state of the Company's cybersecurity and convened a meeting of SolarWinds executives to sound the alarm. Thornton-Trump outlined the steps necessary to remediate these glaring deficiencies and the catastrophic risk the Company faced

[1] Defined terms are the same as in the Consolidated Complaint (the "Complaint") (D.I. 26). Unless otherwise noted, "¶__" refers to Complaint paragraphs, "Mot." refers to Defendants' Motion to Dismiss ("Motion") (D.I. 41), "Thompson Mot." refers to Defendant Thompson's Motion to Dismiss (D.I. 44), "Silver Lake Mot." refers to Defendant Silver Lake's Motion to Dismiss (D.I. 42), "Thoma Bravo Mot." refers to Defendant Thoma Bravo's Motion to Dismiss (D.I. 45), "Biles Decl." refers to the Declaration of Michael J. Biles (D.I. 43), all emphasis has been added, and internal quotes and citations are omitted.

if it failed to act. The executives in attendance agreed with his findings, but all had the same reaction: SolarWinds' then-CEO, Defendant Kevin Thompson, would not spend the money required to create the cybersecurity infrastructure that the Company publicly represented it already had. Thornton-Trump—whose job description included publicly representing SolarWinds' cybersecurity efforts—was unwilling to lie about SolarWinds and, accordingly, resigned in protest.

Because Defendant Thompson refused to address cybersecurity, SolarWinds remained completely vulnerable throughout the Class Period. For example, until November 2019, a malicious actor could have uploaded malware to the Update Server—the server from which SolarWinds customers downloaded software updates—by simply using the password "solarwinds123," as a cybersecurity researcher warned and demonstrated to the Company during the Class Period. Worse yet, the password to this critical Update Server was available on a popular public website as early as 2018—essentially a cyberattack roadmap available to anyone.

In December 2020, SolarWinds revealed that it had been breached. As the Company and media outlets revealed more about the breach, investors learned more about SolarWinds' deficient cybersecurity practices, including that its "solarwinds123" password for its critical Update Server had been publicly available for years. SolarWinds' stock price plummeted, losing 40% of its value in a single week. Both the SEC and DOJ launched investigations into Defendants' misconduct. Media outlets and analysts described the breach as one of the worst in United States history, blaming SolarWinds and the absence of the security controls Defendants assured investors that the Company possessed. "My God," wrote Jody Westby, *Forbes* contributor and CEO of Global Cyber Risk, "[w]e have waited long enough for companies to devote adequate attention and resources to cybersecurity programs. This is the consequence. We must do better … or the bad guys will win."

The Complaint satisfies the pleading requirements for Exchange Act claims. The Complaint details how the Executive Defendants knew or, at minimum, were severely reckless in not knowing, that SolarWinds' representations in the Security Statement and elsewhere were false or, at minimum, materially misleading. Defendant Brown was, by his own account, "responsible for the security of [SolarWinds'] products ... as well as the security for [the Company's] infrastructure," and specifically directed shareholders and the public to the Security Statement when publicly representing the Company. Given how much Defendant Brown professed to know of and spoke about SolarWinds' cybersecurity, he—of all people—knew or, at minimum, was severely reckless in not knowing, that SolarWinds lacked the basic controls specified in the Security Statement. *See In re BP p.l.c. Sec. Litig.*, 843 F. Supp. 2d 712, 783 (S.D. Tex. 2012) (finding compelling inference of scienter where CEO, "as the spokesperson and champion for BP's reform efforts," would have "paid special attention to BP's process safety efforts or, at the least, was reckless in not doing so while continuing to publicly tout improvements").

Faced with the Complaint's well-pleaded allegations, Defendants resort to asserting an alternative set of "facts" that resembles neither the Complaint's allegations nor reality. They impermissibly and misleadingly rely on cherry-picked and disputed "facts" drawn from their 31 exhibits. As discussed in the accompanying opposition to Defendants' footnote request for "judicial notice" and "incorporation by reference," (*see* D.I. 54) their tactic is part and parcel of a "concerning pattern in securities cases" of defendants impermissibly trying to exploit these doctrines to "defeat what would otherwise constitute adequately stated claims at the pleading stage." *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998 (9th Cir. 2018).

Employing their counterfactual narrative, Defendants assert that the cybersecurity deficiencies at issue in the Complaint did not cause the cyberattack. But the Complaint is replete

with allegations to the contrary. *See, e.g.*, ¶154 ("[T]he Company's deficient cybersecurity controls made SolarWinds an attractive and easy target for, and led to, the cybersecurity breach."); *see also* ¶¶157-59, 163. In any event, at best, this dispute about "loss causation"—i.e., what caused investors' losses—merely raises fact issues that cannot be resolved at the pleading stage, particularly because loss causation allegations are subject in this Circuit to Rule 8's liberal pleading standard.

Defendants also try to avoid liability by contending that Defendant Brown did not "make" the Security Statement. But the securities laws impose liability on all corporate executives with "ultimate authority" over the statement, even if they did not write the words. The Complaint pleads that Brown approved, adopted, and had ultimate authority over the Security Statement. By his own account, he was "responsible" for cybersecurity at SolarWinds; he specifically directed customers and investors to the Security Statement in his public statements; and the Security Center page that housed the Security Statement prominently featured a picture of Brown's face with a video by him welcoming investors to "***our*** new security resource center."

Defendants also try to disparage Ian Thornton-Trump, the Company's former Global Cybersecurity Strategist, who alerted the Company's top executives to the absence of cybersecurity controls at SolarWinds. But try as they might, Thornton-Trump is a highly-accomplished expert in cybersecurity, and his Presentation to the Company's top executives—which included several of Defendant Thompson's direct reports—provides strong support for the inference that Defendants were, at minimum, severely reckless in not knowing that the Security Statement was false. That Thornton-Trump was able to identify glaring deficiencies in SolarWinds' cybersecurity controls within months of his joining the Company speaks volumes about just how deficient the Company's cybersecurity actually was.

Defendants contend that it is ***possible*** that everything changed the minute Thornton-Trump left SolarWinds. While anything is theoretically ***possible***, that is not the question on a motion to dismiss. The Complaint's allegations overwhelmingly show that SolarWinds did not clean up its act. An additional ten former SolarWinds employees aver—without exception—that the Company had no security team, no password policy, and no cybersecurity training during the Class Period. Investigative reports from the *New York Times*, *Bloomberg*, and other reputable media outlets all corroborate these accounts, as does the Company's all-too-late "Secure-by-Design" initiative recently put in place by its new CEO to implement the cybersecurity safeguards that SolarWinds falsely told investors it had from the start. Again, at most, Defendants' speculative and counter-factual assertions raise fact issues that cannot be resolved at the pleading stage.

Investors have suffered immensely as a result of Defendants' misrepresentations. SolarWinds' stock price has never recovered since the revelations about its deficient cybersecurity controls; its customers have fled in droves; and the SEC's and DOJ's investigations into Defendants' misconduct remain ongoing. Meanwhile, Defendant Thompson received a $23.9 million bonus for 2020 alone and he, along with the private equity firms that control its operations, reaped over $730 million in stock sales executed just days before investors learned the truth.

Defendants' motions should be denied, and the factual disputes resolved through discovery.

II. FACTUAL BACKGROUND

SolarWinds sells network software. At the start of the Class Period, SolarWinds and the two private equity firms that controlled it—Defendants Thoma Bravo and Silver Lake—took the Company public and sold $635 million of shares to outside investors. ¶28. As part of these offerings and later sales, the two private equity firms reaped large profits. All the while, they maintained an iron-clad grip over SolarWinds' activities, insisting upon a cost-cutting strategy that prioritized short-term profits over all else—including the security of SolarWinds customers. *Id.*

A. SolarWinds Gains Prominence In The Federal Government And Beyond

Both before and during the Class Period, SolarWinds courted federal government agencies as customers. The government contracting business is extremely lucrative, with over $430 billion directed towards contracts for services and goods each year. ¶29. Government agencies require security and expect their vendors to maintain strict cybersecurity controls. As the Deputy National Security Advisor for Cyber and Emerging Technology explained, "the government, and indeed all consumers, don't have visibility into what software is developed securely, and what's not…. [W]e put our trust in vendors, but we do it blindly for the most part, because we don't have a way to measure that trust." ¶30.

To gain prominence in the software market for government agencies, SolarWinds needed to convince them that cybersecurity was a top priority for the Company. At every turn, SolarWinds emphasized that it was singularly focused on cybersecurity. In touting its capabilities in its "SolarWinds Government White Paper," the Company stressed that it "can help federal agencies with … basic cyber hygiene," assuring federal agencies that "SolarWinds has the tools, expertise, and experience-based knowledge of the federal space to help any agency enhance its security posture, reduce risk, and more effectively protect agency data." ¶31.

On May 22, 2018, the Company issued a press release announcing the launch of its "Security Resource Center—a one-stop shop for the latest security news and resources." ¶32. The "Security Resource Center" purported to provide "the information ... need[ed] about current security issues and trends, as well as recommended best practices to help ensure their business and customers are protected." *Id.* The Company highlighted that its "Security Resource Center will provide real-time alerts and important information from the field, including 'How-to Guides.'" *Id.* The Company's press release also emphasized that it would begin issuing "The Brown Report," a regular report authored by Defendant Brown, "which looks at the latest cybersecurity threats that

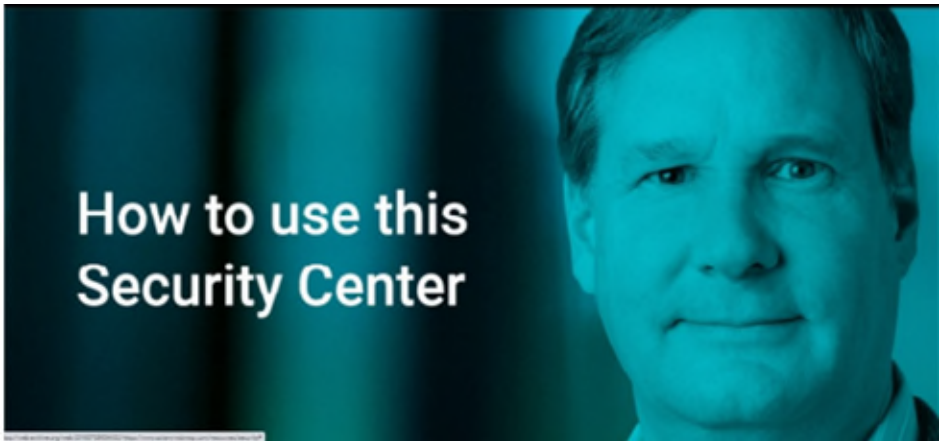
may impact [managed service providers], and tackles each topic with an eye toward actions [managed service providers] can take today to help stay ahead of threats and help keep their clients safe from cyberattacks." *Id.* The Company's press release announcing its "Security Resource Center" quoted Defendant Brown, who urged customers and investors to come visit the SolarWinds Security Center. *Id.*

Defendant Thompson also stressed to investors the bleak cybersecurity threat landscape and SolarWinds' ability protect even small businesses. For example, during an investor conference, Defendant Thompson emphasized that "the threat landscape is getting worse, not better," stating that "every small business [] actually has a heightened level of sensitivity right now to security issues because the reality is if the small business gets hacked, they go out of business." ¶33. He highlighted SolarWinds' ability to capture market share because its software purportedly gave "small businesses around the world the ability to protect themselves." *Id.*

Defendants' tactics worked. Investors and customers believed that SolarWinds was laser focused on cybersecurity and maintained strict controls to protect their clients' data. As a result, the Company amassed over 300,000 customers worldwide and obtained contracts with the United States government totaling more than $230 million. ¶34. The Company's customers included (i) all five branches of the U.S. Military, (ii) the U.S. Pentagon, State Department, NASA, NSA, Department of Justice, and the Office of the President of the United States, (iii) the FBI, Secret Service, National Nuclear Security Administration, and the Department of Homeland Security, (iv) more than 425 of the U.S. Fortune 500 companies, (iv) the top ten U.S. telecommunications companies, and (v) the top five U.S. accounting firms. *Id.* As a result of its ability to attract this clientele, SolarWinds' stock price soared, and it was on track to generate $1 billion in revenue by the second quarter of 2020. *Id.*

B. SolarWinds Assures Customers And Investors That It Adheres To Its "Security Statement" And Is Committed To Cybersecurity

Throughout the Class Period, SolarWinds and its top executives detailed their purported adherence to cybersecurity in a formal Security Statement, which appeared prominently on, and was accessible from every page of, the Company's website. ¶37. The Security Statement, which was reviewed and approved by Defendants Brown and Thompson, first appeared on the Company's website on or about August 28, 2018, and was permanently featured on the website throughout the Class Period. *Id.* The Company's "Security Center" page, which included the Security Statement, included the below picture of Defendant Brown, who welcomed investors and customers in an accompanying video in which he stated, "I'm excited to share ***our*** new security resource center with everyone." ¶38.



In the Security Statement, Defendant Brown and SolarWinds made a series of representations about their purported adherence to cybersecurity practices, including that the Company: (i) had a dedicated Security Team with well-defined roles (¶43); (ii) had an Information Security Policy that the Company purportedly required employees to sign and acknowledge (¶45); (iii) required all new employees to participate in security training (¶47); (iv) had a Password Policy covering all employees and all Company systems, applications, and databases (¶49); (v) restricted employee access to Company resources based on their job function, limiting access to "sensitive

data" on a "need-to-know basis" (¶52); (vi) segmented its network, maintaining "separate development and production environments" (¶55); and (vii) adhered to the NIST Cybersecurity Framework, including the requirement that background checks be conducted on all prospective employees (¶57).

SolarWinds executives frequently directed investors and customers to the Company's website and Security Center, and specifically the Security Statement. ¶¶39-41. For example, in Defendant Brown's article posted on the Company's website, "Do Your Vendors Take Security Seriously?," he underscored the importance of software companies publishing their cybersecurity statements. ¶39. He stressed that "importantly, strong vendors publish their security protocols and processes so you can evaluate whether they meet your standards" and "reiterate[d] the point … [that] your vendors should [] publish their policies and protocols." *Id.* He then directed investors and customers to SolarWinds' Security Statement located in its "Trust Center," telling readers that they "can learn all about the steps we take to protect your data by visiting our Trust Center today." *Id.*

C. Unknown To Investors At The Time, SolarWinds' Internal Security Was In Shambles And The Company Did Not Adhere To Its Security Statement

Unknown to investors at the time, SolarWinds was ***not*** committed to cybersecurity and failed to put into place ***any*** of the critical and basic cybersecurity safeguards that it assured customers and investors it had implemented. Instead, Defendant Thompson and the Private Equity Firms that controlled SolarWinds were myopically focused on cost-cutting to achieve near-term gains and meet analysts' quarterly revenue estimates.

1. SolarWinds Executives Were Told About The Company's Deficient Cybersecurity Controls

Shortly before the Class Period, Ian Thornton-Trump—a 15-year veteran of the cybersecurity industry and SolarWinds' Global Cybersecurity Strategist—alerted the Company

and several of its top executives to cybersecurity deficiencies at the Company.

Lead Counsel spoke with Thornton-Trump. He stated that "[t]here was no corporate security" at SolarWinds and no dedicated security positions at all at SolarWinds. ¶66. He further explained that, at SolarWinds, there was no Chief Information Security Officer ("CISO")—a standard security position at software companies handling customer data. *Id.* He additionally described how there was no person centrally coordinating security efforts at SolarWinds and that, in addition to lacking a corporate security department, there was no process for ensuring the Company's software products were secure. *Id.* The absence of a security team was especially surprising to Thornton-Trump, as the risk of the Company being hacked was well known. *Id.*

Thornton-Trump identified other critical deficiencies in cybersecurity at SolarWinds. When he asked his colleagues at SolarWinds for documentation regarding cybersecurity, they could not provide any. ¶67. He reiterated that he never saw any written information security policy at the Company, adding that that there was no cybersecurity training at SolarWinds. *Id.* He also observed that the Company was not protecting its employees' computers from attack and that workstation vulnerabilities were not addressed at SolarWinds. ¶69.

Even more, Thornton-Trump explained that SolarWinds did not limit its employees' user access controls on its critical networks, exposing the Company's "crown jewels"—its most sensitive assets. ¶70. There were no restrictions or controls in place regarding network segmentation. *Id.* Development engineers' network areas should have been segmented, with heightened security from the rest of the network, but they were not. *Id.* To the contrary, SolarWinds was using a "flat" network, which meant anyone at the Company could connect to any server in the network; rather than allowing a very small group of people access to the Company's "crown jewels," it was a free-for-all. *Id.*

Thornton-Trump further described that SolarWinds also did not follow any password policies, with employees using highly vulnerable passwords. ¶71. Compounding matters, for the development portions of the network, there was no password change policy—meaning that passwords could remain the same indefinitely. *Id.* As a result, some of the passwords in the development unit of the business were "hard-coded," such that they could never be changed; if the passwords were changed, the product would stop working. *Id.* Based on his vast experience, work at the Company, and review of its practices, Thornton-Trump concluded that, "from a security perspective, SolarWinds was an incredibly easy target to hack." ¶72.

Thornton-Trump voiced his concerns to the Company's executives. When his concerns were not taken seriously, Thornton-Trump decided that he needed to make the case for security at SolarWinds more forcefully. In advance of doing so, Thornton-Trump conducted approximately one month of research, "d[ug] pretty deep" and spoke to people about active attacks in the cybersecurity space. ¶73.

On or about April 22, 2017, Thornton-Trump convened a meeting with several of SolarWinds' top executives. ¶74. Attendees included SolarWinds' Chief Technology Officer, Joe Kim; Chief Information Officer, Rani Johnson; and Chief Marketing Officer, Gerardo Dada. *Id.* Messrs. Dada and Kim both reported directly to Defendant Thompson. *Id.* At the meeting, Thornton-Trump presented a PowerPoint Presentation titled "Creating Security." *Id.*

During his Presentation, Thornton-Trump stressed to the Company's executives that "[w]e need to be good cyber security citizens," explaining that a "data breach is bad for us and bad for our customers." ¶75. Thornton-Trump started his Presentation by explaining his findings to the Company's executives that, with regard to cybersecurity, there was ***"No centralized reporting," "No centralized management,"*** and ***"Silos of communication."*** *Id.*

To remedy these problems, Thornton-Trump explained to the Company's executives that SolarWinds needed to develop a security team. ¶76. Specifically, he told them that the Company needed, at minimum, to hire a CISO, a Senior Director of Cyber Security, and two Portfolio Security Managers. *Id*. Thornton-Trump stressed that a security team was necessary to avoid a catastrophic cyberattack. As he stated point-blank, SolarWinds' ***"infrastructure and corporate systems exist in a precarious state."*** ¶77.

Thornton-Trump further told the Company's executives, including Defendant Thompson's direct reports, that this precarious state, if not rectified, would result in another cyberattack. *Id.* He reminded his colleagues that the Company had already been subjected to the "Apache Struts" compromise, a damaging security breach during which "cyber criminals quickly exploited" and compromised "over 500 customer systems." *Id.*

Thornton-Trump's Presentation made abundantly clear that significant and immediate reform was necessary. He explained that a commitment to cybersecurity was essential to the Company's continued existence. He stated: ***"The survival of our customers depends on a commitment to build secure solutions"*** and ***"The survival of the company depends on an internal commitment to security."*** ¶80.

The executives in attendance at his Presentation, including Defendant Thompson's direct reports, all agreed with Thornton-Trump's assessment of the state of cybersecurity at SolarWinds and what needed to be done to remedy the situation. ¶81. Thornton-Trump explained that they agreed that cybersecurity was a problem at SolarWinds and knew it was getting worse. *Id.* Indeed, none of the SolarWinds executives in attendance knew who owned security of the Company's development operations. ¶82. And when Thornton-Trump asked Joe Kim, Defendant

Thompson's direct report, why SolarWinds did not have any development operations security, Kim admitted that ***"[w]e're just not there yet."*** *Id.*

Thornton-Trump explained that he saw his Presentation to SolarWinds' executives as an opportunity to save the Company—as he explained, it was "clear as day" that a cyberattack was coming. ¶83.

2. SolarWinds Refuses To Reform, Causing Its Global Cybersecurity Strategist To Resign In Protest

Thornton-Trump's Presentation was widely discussed within SolarWinds. ¶84. But because Defendant Thompson did not want to spend money on cybersecurity, Thornton-Trump's remediation plan was rejected. ¶85. Thornton-Trump explained that, when he delivered his Presentation, he was met with resistance as to costs because that was the corporate culture at SolarWinds. *Id*. Defendant Thompson's two highest-ranking direct reports, Gerardo Dada and Joe Kim, both told Thornton-Trump that Thompson would not spend money on security, and an attendee at the Presentation stated that "Kevin [Thompson] won't like spending that kind of money"—a statement that none of the other SolarWinds executives in attendance disagreed with. *Id.* "Everyone understood the risk [of not addressing cybersecurity] … but it just wasn't going to happen," Thornton-Trump added. *Id.*

Following his "Creating Security" Presentation, Thornton-Trump was notified that the Company's senior leadership was, in fact, not interested in spending the money to implement the necessary changes outlined in the Presentation. ¶86.

Thornton-Trump resigned in protest. ¶87. He explained that he did not want to be put in a position where he was asked to say something publicly about SolarWinds' cybersecurity that was not the truth. *Id*. He conveyed the reasons for his departure at the time to his fellow SolarWinds executives. Thornton-Trump emailed Defendant Thompson's direct report, Mr. Dada,

about the reasons for his resignation. He wrote that "[u]nfortunately … the current SW [Solar Winds] MSP leadership is … unwilling to make the corrections necessary," which Thornton-Trump noted was "[a] point I made in my briefing to the [Chief Information Officer]." ¶88. He explained that he had "lost faith in the leadership" of the Company, and that it was "too painful to watch from the sidelines as mistake after mistake unfolded." *Id.* Dada did not disagree with Thornton-Trump's assessment of the Company's failures. To the contrary, Dada responded to Thornton-Trump's email that he "***agree[d] with [his] assessment*** and … appreciate[d] the effort and candor [he] put behind trying to do the right thing at SolarWinds." ¶89.

3. SolarWinds Lacked The Cybersecurity Protections That It Represented In Its Security Statement Throughout The Class Period

Ten former SolarWinds employees have confirmed Thornton-Trump's account and that Defendants did not remedy SolarWinds' cybersecurity deficiencies during the Class Period. As the *New York Times* would later explain, SolarWinds' "former employees and advisers" knew that "SolarWinds was a ripe target [for a cybersecurity attack] not only for the breadth and depth of its software, but for ***its own dubious security precautions***." ¶113. *Bloomberg News* similarly explained, based on its investigation, that "several cybersecurity researchers … discovered what they described as ***glaring security lapses at the company***." *Id.* Contrary to its public representations, SolarWinds failed to adhere to the representations in its Security Statement, exposing its customers to a cyberattack and investors to major losses.

SolarWinds had no "Security Team." The Company's Security Statement assured investors that SolarWinds employed a dedicated "security team," with "[i]nformation security roles and responsibilities … defined within the organization." ¶114. But, in truth, the Company lacked any such "security team." *Id*. As Thornton-Trump explained, security roles were not

defined within the organization; the Company had no security leadership, no security team, and no centralized way of dealing with security at a corporate level. *Id*.

Several former SolarWinds employees have explained that nothing changed after Thornton-Trump's resignation. FE 2 confirmed that, during his six years at the Company, he never once heard of a security team at the Company. ¶115. FE 4 likewise stated that, in the nearly six years he worked at the Company, he never heard of a security team at SolarWinds. *Id.* FE 5 confirmed that that there was no cybersecurity team at SolarWinds. ¶95. FE 7, who sold the Company's security-focused products for years, recounted that he was never told about a security team at the Company and stated that, if such a team existed, he believed he would have interfaced with them. *Id.* FE 6, who was at the Company for nearly three years, confirmed he was not aware of any security team at SolarWinds. ¶¶97 n.26, 115. Additionally, the *New York Times* noted, in its December 16, 2020 exposé, that the Company ***still*** had not hired a CISO—the critical executive position tasked with overseeing cybersecurity that Thornton-Trump flagged as a serious vacancy three years earlier. ¶115.

SolarWinds had no "Security Information Policy." The Security Statement also represented that SolarWinds maintained a Security Information Policy and required its employees to review and sign such a policy. ¶116. But no such policy existed, and employees were never required to sign such a policy. ¶¶117-18. Thornton-Trump explained that he never saw an information security policy, and there was no documentation that he received that discussed SolarWinds' data protection policies or controls. ¶117.

The situation did not change after Thornton-Trump's departure. FE 2 was familiar with the Company employee manual and confirmed that there was no information about a security policy during the Class Period. ¶118. He did not recall ever receiving a security policy at

SolarWinds; nor did he recall being required to sign any such policy, including at the time he was hired. *Id.* FE 4 likewise stated that, in his nearly six years at the Company, he never saw or received a written information security policy, and never had to sign any document about cybersecurity. *Id.* FE 5 confirmed that, when new employees joined the Company, there was no cybersecurity agreement that they had to sign, and FE 5 stated that he never signed any such agreement in his time at the Company. *Id.* FE 10 added that he looked back through the documents he was given when he was onboarded as a SolarWinds employee and saw nothing about internal information security. *Id.*

SolarWinds did not have or follow a "Password Policy." SolarWinds assured investors in its Security Statement that the Company adhered to a strict password policy, with the Company purportedly employing "password best practices [that] enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords." ¶¶49, 119. In truth, as Thornton-Trump and others have described, the Company did not have a password policy, did not employ password best practices, and instead used hard-coded default passwords that were compromised. ¶¶119-22.

Multiple former employees of the Company confirmed that SolarWinds neither maintained nor adhered to a password policy during the Class Period. ¶120. With no password policies in place, SolarWinds' critical systems were accessible using a hard-coded default password that never changed and was remarkably easy to guess: "solarwinds123." ¶122. This password was used to access SolarWinds' critical Update Server, as well as to access other important systems and networks within the Company. ¶123.

SolarWinds did not provide cybersecurity training to its employees. SolarWinds further represented in its Security Statement that the Company provided its employees with cybersecurity

training. ¶125. In reality, SolarWinds never did. ¶¶125-30. Thornton-Trump explained that, while he was at the Company, there was no cybersecurity awareness education or training at SolarWinds at all. ¶125.

Nothing changed on this front during the Class Period. SolarWinds former employees explained that they never received any cybersecurity training at SolarWinds during the Class Period. FE 2, who was with the Company from 2014 until July 2019, stated that security trainings did not exist at SolarWinds. ¶126. FE 3 confirmed that he also could not recall ever receiving a security training course at SolarWinds. ¶130. FE 4 similarly stated that there was no security training at SolarWinds during his entire tenure with SolarWinds—from 2016 to June 2020. ¶127. FE 5 also confirmed that SolarWinds never did any internal cybersecurity training. ¶128. FE 7 also confirmed that there was no security training at SolarWinds. ¶129. FE 8 also confirmed that there was no security training at all at the Company. ¶130. FE 9, who was with the Company for five years, similarly confirmed that there was no cybersecurity training at the Company during his tenure at the Company. *Id.* And FE 10 likewise confirmed that he received no cybersecurity training whatsoever at SolarWinds. *Id.*

SolarWinds did not segment its network. The Company's Security Statement also stated that SolarWinds restricted employees' access within the Company's network, which was supposedly "segmented" in order to prevent and mitigate harm in the event of a cyberattack. ¶¶55, 131. In truth, the Company's network was not segmented, and SolarWinds employees were allowed unfettered access to critical databases and information areas. ¶¶131-36. Thornton-Trump explained that the workspace for development engineers should have been segmented with heightened security, but that was not occurring at SolarWinds. ¶132. He explained that the

Company was using a "flat" network, which meant anyone could connect to any server on the network. *Id.*

SolarWinds' practices did not change during the Class Period. FE 2 stated that employees who were not in development operations could access parts of the development operations system. He knew this because he did so personally. ¶133. He confirmed that there was an absence of limitations on user access. *Id.* When asked if there were controls over where users could look within the SolarWinds network, FE 4 confirmed there were no restrictions and that he could view other products that he did not work on. ¶134. FE 10 similarly stated that employees' access to the network was a "free for all"—he was able to access files above his level and never saw any restrictions on Company computers. ¶135.

SolarWinds did not perform background checks on its employees. The Company's Security Statement also assured investors that the Company "follows the NIST [National Institute of Standards and Technology] Cybersecurity Framework," which includes a requirement to conduct employee background checks. ¶57. This too was false. FE 5, the Company's director of global recruiting, explained that the Company did not do background checks on candidates for any employment position. ¶138. In fact, FE 5 was spearheading the effort to implement background checks for employment candidates, but the reform still was not implemented by the time he left the Company after the Class Period. *Id.* FE 6, who also worked in human resources at SolarWinds, likewise confirmed that SolarWinds did not do background checks on new hires, and it was a general concern that they were not being done. ¶139.

4. SolarWinds Is Told That The Password To Access Its Internal Update Server Was Publicly Available On The Internet For Years

The grave consequences of SolarWinds' failure to adhere to its cybersecurity commitments were made even more apparent on November 11, 2019. On that date, a researcher, unaffiliated

with SolarWinds, notified the Company in writing that the supposedly confidential password to access, modify, and add files to its Update Server was ***publicly available*** on a website.

By way of background, SolarWinds—like most software companies—maintains an update server on its website. ¶104. SolarWinds directed customers to visit its Update Server to download updates to Company software that customers purchased. *Id.* SolarWinds employees need a password to access and add files to the Update Server. *Id.* It is critical that the password to the Company's internal server to add files to the Update Server is kept confidential and secure, so as to avoid malicious materials being added to the Update Server for download by customers. *Id.*

Unknown to customers and investors until the final day of the Class Period, SolarWinds' Update Server was compromised for approximately ***one-and-a-half years***. ¶105. On June 17, 2018, a SolarWinds employee posted the credentials and a link to the Update Server on a popular public website, GitHub. *Id.* The credentials and link enabled ***anyone*** to enter SolarWinds' Update Server. *Id.* By accessing SolarWinds' internal system using the password and credentials on the public GitHub website, ***anyone*** could add malware to any of the update files that the Company sent out to its tens-of-thousands of customers, including U.S. federal agencies. *Id.*

On November 19, 2019, Vinoth Kumar—a software engineer who specializes in security—notified SolarWinds in writing of this critical compromise to its Update Server. ¶106. Kumar told SolarWinds that he "found a public GitHub repo [i.e., website] which [is] leaking ftp credentials belong[ing] to SolarWinds." ¶107. He directed the Company to the link to the public GitHub webpage that contained the compromised password and user credentials. *Id.* The GitHub webpage provided a link to the Company's internal connection to the Update Server, as well as the "confidential" username and password to access the internal server. *Id.* With these credentials, Kumar (or anyone else) could upload malware or any other file to the Company's Update Server,

which would then be included in the Company's routine software updates downloaded by SolarWinds' unsuspecting customers. *Id.*

To underscore the significance of the Company's egregious cybersecurity failure, Kumar demonstrated to SolarWinds that he had utilized the compromised credentials by entering the Company's Update Server and uploading a file onto it. ¶108. The file that Kumar uploaded would, absent remediation, be included in any updates downloaded by SolarWinds' customers. *Id.* Kumar made the point abundantly clear in his email to the Company, in which he stated that ***"any hacker could [have] upload[ed] malicious [files]"*** onto the SolarWinds Update Server. *Id.*

Kumar's email to SolarWinds included the Company's password for its internal access to the Update Server. The password was "solarwinds123," an obviously vulnerable password that violated basic password policies. ¶109. Remarkably, the Company had tasked an intern to set the password for this critical Update Server. *Id.* Worse yet, the Company's intern set the password for this critical server in 2017—meaning that a compromised password for SolarWinds' critical Update Server remained unchanged for ***over two years***. *Id.*

The implications of the Company's public dissemination of its password to its Update Server were plain. ¶110. Kumar later recounted to *Reuters* that ***"anyone could access SolarWinds' update server by using the password 'solarwinds123.'"*** *Id.* As he further explained, ***"'[t]his could have been done by any attacker, easily.'"*** *Id.*

Defendant Brown admitted in March 2021 interviews that he had contemporaneous knowledge that the password to the critical Updater Server was compromised and—recognizing the significance of this fact—changed the password for the server on the same day he received notification. ¶112. Investors and customers, however, were kept in the dark. No action was taken to advise investors that the Company's Update Server had been compromised for one-and-a-half

years, with its password publicly available for anyone to use and download malicious software. *Id.* Nor were investors ever told that SolarWinds lacked the most basic of cybersecurity policies, procedures, and practices represented in the Security Statement. *Id.*

D. The Truth About The Company's Deficient Cybersecurity Emerges

On Sunday, December 13, 2020, a series of media reports revealed that cybercriminals had inserted malware into the software distributed to SolarWinds' customers through the Update Server. ¶150. A United States government official identified the breach as "the worst hacking case in the history of America." *Id*.

SolarWinds did not disclose the breach; rather, reports of the breach first emerged via reporting by *Reuters*. ¶151. The Company's infected software updates were downloaded by customers for over six months and by tens-of-thousands of SolarWinds' customers, including U.S. government agencies and Fortune 500 companies. *Id.* Once downloaded by SolarWinds' customers, the infected software enabled the cybercriminals to spy on them. *Id.* The cybercriminals could access SolarWinds' customers' classified documents, review their private emails, and obtain their trade secrets. *Id.* Worse yet, the Company has admitted that the cybercriminals entered the Company's network beginning ***two years earlier***—i.e., while the password to its Update Server was publicly available and compromised. ¶152.

Over the subsequent days and weeks following the revelation of the SolarWinds breach, reports emerged further demonstrating SolarWinds' deficient cybersecurity controls. ¶¶153-67. These revelations caused the Company's stock price to decline by a total of 40%. ¶162.

Among other revelations, on December 15, 2020, public reports emerged that (as discussed above at pages 18-20) the password to access the Company's Update Server was "solarwinds123" and had been on a public website for a year-and-a-half. ¶157. Cybersecurity experts recognized that the Company exhibited deficient cybersecurity controls by (1) allowing its employees to

utilize the password "solarwinds123" to upload the updates to the Update Server; (2) never changing the password for over two years; (3) authorizing an intern to set this critical password and access the Update Server; and (4) enabling the password to enter the public domain for over one-and-a-half years without ever being addressed. *Id.*

SolarWinds' use of the password "solarwinds123" for a critical server was, as Professor Terry Thompson of John Hopkins University explained, "an egregious violation of fundamental standards of cybersecurity." ¶158. SolarWinds' explanation—that the password was set by an intern—further demonstrated the Company's failure to adhere to basic cybersecurity practices. *Id.* As the executive director of security at Okta, Marc Rogers, explained, "[i]n placing blame on an intern for setting a production password in 2017 …, SolarWinds revealed deep, systemic cybersecurity failures at many levels of the organization…. That intern's ability to set a password of 'solarwinds123' on a critical production system highlights fundamental problems with password policy, systems management and auditing…. All of these failures suggest an organization rife with systemic security issues, an ineffective security management program, and a lack of technical controls or compliance with industry standards." *Id.* Rogers further commented that organizations, such as SolarWinds, "that allow junior employees privileged access to production systems like this are typically a 'Wild West' when it comes to controlling access for all systems, not just one." *Id.* In an article titled "SolarWinds Cyber Attacks Raise Questions About The Company's Security Practices And Liability," *Forbes* contributor and CEO of Global Cyber Risk, Jody Westby summed it up, "We have waited long enough for companies to devote adequate attention and resources to cybersecurity programs. ***This is the consequence.***" ¶159.

Days later, additional major media outlets published investigative reports that included first-hand accounts of current and former SolarWinds employees. These reports further confirmed

the deficiencies in the Company's cybersecurity controls. The reports included the account of, among others, Thornton-Trump, who explained that SolarWinds' cybersecurity deficiencies rendered the Company an "easy target to hack." ¶163. Commentators took note, such as Jake Williams, a former employee of the NSA. He explained that security deficiencies were an "underlying problem" at SolarWinds that remained because the Company viewed "'[s]ecurity as a cost center, not a profit center.'" *Id.* Professor Terry Thompson likewise concluded that ***"SolarWinds, driven by its growth strategy and plans to spin off its managed service provider business in 2021, bears much of the responsibility for the damage."*** *Id.* David Corchado of Investis Digital echoed that the breach should serve as a "wake-up call" that SolarWinds had deficient security practices. *Id.*

The fallout from the cybersecurity breach continues and has been immense. Thomas Bossert, the homeland security adviser to President Trump and the deputy homeland security adviser to George W. Bush, wrote in the *New York Times* that SolarWinds allowed the cybercriminals "persistent access" to the networks they infiltrated, meaning they could continue to access the networks. ¶165. As he explained, "The remediation effort alone will be staggering. It will require the segregated replacement of entire enclaves of computers, network hardware and servers across vast federal and corporate networks." *Id.*

Since the revelation of SolarWinds' deficient security practices, SolarWinds has become the laughingstock of the software industry. ¶167. Trust in SolarWinds has eroded, and the Company has lost numerous customers. For the first quarter of 2021, license revenue declined by 33% compared to the first quarter of 2020, with the decrease in renewals led by federal agency customers. ¶166. The Company's stock price has never recovered. ¶167.

E. SolarWinds Is Forced To Admit It Lacked Sufficient Security Measures During The Class Period

SolarWinds has since replaced Defendant Thompson with a new CEO, Sudhakar Ramakrishna, and assured customers and investors that it will now implement the reforms necessary to address the rampant cybersecurity failures that existed at the Company throughout the Class Period. ¶168. This belated suite of reforms—the "Secure-by-Design" initiative—further makes clear that the Company lacked basic cybersecurity measures, including several measures that the Company affirmatively represented it had, during the Class Period. *Id.*

Cybersecurity experts have rightfully taken the Company's belated adoption of these measures as an admission that its cybersecurity was deficient during the Class Period. As *NPR* wrote, ***"the overhaul of SolarWinds' security practices add up to an admission that something was wrong."*** ¶169. Thornton-Trump similarly observed, "[i]f I come up with an 11-point plan to improve my company's security one interpretation of that could be … that there were at least 11 material deficiencies in the actual security we had. I see that the 11-point plan is actually an admission that things were not good in this security house." *Id.* And the Company's new CEO, when asked if the Company could "do thing[s] better" on the cybersecurity front, himself admitted, ***"[a]bsolutely."*** *Id.*

The Company has finally committed to: (i) investing in developing a "security team" of the type that it assured investors in the Security Statement that it had (¶171); (ii) introducing a password policy, including "updating all passwords" and requiring the use of multi-factor authentication to protect against weak passwords, despite its representation in the Security Statement that it already followed a robust password policy (¶173); (iii) enforcing "least privileges policies for ALL employees," demonstrating the falsity of the Company's Security Statement representation that it granted employees "a limited set of default permissions" to the Company's

network (¶174); and (iv) segmenting its network, despite its Security Statement representation that the Company already segmented its network (¶175).

F. The SEC, DOJ, And State Attorneys General Launch Investigations Into SolarWinds, But The Company Still Pays Its Executives Lavishly

SolarWinds' misconduct has spurred a spate of government investigations. The Company has stated that it is facing "numerous investigations and inquiries by domestic and foreign law enforcement and other governmental authorities … including … the Department of Justice, the Securities and Exchange Commission, and various state Attorneys General." ¶177.

While investors have suffered immensely, Defendants profited handsomely. During 2020 alone, the Company paid $23.9 million in bonus payments to Defendant Thompson and another $8.8 million to the Company's former Chief Technology Officer, Joe Kim—one of Thompson's direct reports who Thornton-Trump urged to adopt the directives in his "Creating Security" Presentation. ¶179. As market observers have noted in dismay, "SolarWinds paid its top leaders more than $65 million in total [during 2020] despite a colossal breach that exposed 18,000 customers." *Id.*

III. ARGUMENT

"When faced with a Rule 12(b)(6) motion to dismiss a § 10(b) action, courts must, as with any motion to dismiss for failure to plead a claim on which relief can be granted, accept all factual allegations in the complaint as true." *Lormand v. US Unwired, Inc.*, 565 F.3d 228, 232 (5th Cir. 2009). Motions to dismiss securities actions are "viewed with disfavor and are rarely granted," and courts "must also draw all reasonable inferences in the plaintiff's favor." *Id.* "[I]n the context of securities fraud, a dismissal pursuant to Rule 12(b)(6) is difficult to obtain since such a claim revolves around fact-specific inquiries." *Brody v. Zix Corp*., 2006 WL 2739352, at *2 (N.D. Tex. Sept. 26, 2006). "The sole issue before the Court at this time is whether the claims in Plaintiff's

Complaint are adequately *alleged*, not whether the claims are likely to survive a motion for summary judgment following discovery." *Georgia Firefighters' Pension Fund v. Anadarko Petroleum Corp.*, 514 F. Supp. 3d 942, 957 (S.D. Tex. 2021) (emphasis in original).

A. The Complaint Adequately Alleges False And Misleading Statements

To allege falsity, Lead Plaintiff need only "specify the statements contended to be fraudulent, identify the speaker, state when and where the statements were made, and explain why the statements were fraudulent." *Barrie v. Intervoice-Brite, Inc.*, 397 F.3d 249, 256 (5th Cir. 2005). "Whether or not any of these allegations can be proven during later stages of this litigation" is not relevant to the inquiry. *Spitzberg v. Houston Am. Energy Corp.*, 758 F.3d 676, 691 (5th Cir. 2014). Lead Plaintiff has amply satisfied the pleading requirements here.

1. Defendants Falsely Told Investors That SolarWinds Followed The Practices Set Forth In The "Security Statement"

As detailed in the Complaint, Defendants represented to investors throughout the Class Period that SolarWinds adhered to the specific cybersecurity practices identified in its Security Statement prominently featured on its website. ¶¶42-60. SolarWinds told investors that it maintained a dedicated "security team" (¶43), required employees to sign an "information security policy" (¶45), provided security training to all employees (¶47), enforced stringent password policies (¶49), segmented the Company's network and limited user authorization (¶¶52, 55), and adhered to the NIST Cybersecurity Framework's requirements, which includes background checks on employees (¶57).

Not one of these core representations in the Security Statement was true. In reality, the Company lacked each of these critical cybersecurity practices and protections. ¶¶113-39. SolarWinds' employees uniformly described how the Company had ***no*** security team (¶114-15), ***no*** information security policy (¶117-18), ***no*** cybersecurity training (¶¶126-30), ***no*** password

policy (¶¶120-24), and ***no*** controls that limited employees from accessing its "crown jewels" (¶132). Both before and after Thornton-Trump's resignation, SolarWinds (i) permitted the use of default and hard-coded passwords for systems, including the critical Update Server; (ii) allowed unfettered employee access to all areas of the network without regard for their individual roles in the organization; and (iii) failed to perform basic background checks of employees. *See* ¶¶71, 96, 99, 121, 132-33.

Misrepresentations about a company's security practices—such as those contained in the Security Statement—are actionable, as courts have repeatedly found. For example, in *In re Equifax Inc. Securities Litigation*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019) ("*Equifax*"), the court held defendants liable for having falsely represented before a cyberattack that they had "used 'a variety of technical, administrative and physical ways to keep personal credit data safe'" and "'regularly review[ed] and update[d] [the] security protocols.'" *Id*. at 1222. Likewise, in *Bricklayers & Masons Local Union No. 5 Ohio Pension Fund v. Transocean Ltd.*, 866 F. Supp. 2d 223 (S.D.N.Y. 2012), the court held defendants liable for having falsely represented before an oil spill that the company had "conducted 'extensive' training and safety programs." *Id*. at 243. And similarly, in *In re BP p.l.c. Securities Litigation*, 843 F. Supp. 2d 712 (S.D. Tex. 2012), the court held BP liable for having falsely stated before an oil spill that it had taken certain steps to make "progress in process safety" when in reality, it had not. *Id*. at 757.

In response to the Complaint's well-pled allegations, Defendants make a host of fact-intensive arguments. Each of them fails.

First, SolarWinds urges the Court to ignore the Complaint's well-pled allegations and instead adopt SolarWinds' say-so, much of which is impermissibly drawn from cherrypicked extrinsic documents. *See* Lead Pl's Opp'n to the SolarWinds Defendants' Footnote Request for

Judicial Notice or Incorporation-by-Reference of 31 Exhibits (D.I. 54). Far from an "innocent cybersecurity victim," SolarWinds put its customers, the federal government, and the country in grave danger through its stunning failure to adhere to the most basic cybersecurity practices detailed in the Security Statement. Precisely because of SolarWinds' misrepresentations, Defendants are currently under investigation by the SEC, the DOJ, and dozens of state Attorneys General; SolarWinds' stock price lost 40% of its value; it has lost numerous customers; and its "solarwinds123" password for its Update Server has marred the Company's reputation. This is not a baseless "event driven" lawsuit, as Defendants would have the Court believe; rather, it is the direct result of SolarWinds' false and misleading statements to the market, and the Complaint is the product of an extensive investigation backed by 11 witness accounts as well as investigative reports published by the *New York Times*, *Bloomberg*, and cybersecurity experts around the globe.

Defendants' version of events—in which the Complaint is factually wrong and they had the represented cybersecurity controls in place—also cannot be squared with the announcement of SolarWinds' "Secure-by-Design" initiative. Under the "Secure-by-Design" initiative, the Company ***now***—three years after its publication of the Security Statement—finally intends to establish a dedicated security team, review the Company's password management policies, enforce limited access privilege policies, and segment its networks. ¶¶171-76. That the Company announced an initiative introducing needed cybersecurity practices and policies provides further evidence that the Company did not have those practices and policies in the first place. *See Plotkin v. IP Axess Inc*., 407 F.3d 690, 698 (5th Cir. 2005) ("[A]llegations of later-emerging facts can … provide warrant for inferences about an earlier situation.").

Second, Defendants assert that their boilerplate "risk" warning of a possible future cyberattack in a 229-page SEC filing gave them license to lie in the Security Statement about their

actual cybersecurity practices. *See* Mot. at 32. They are sorely mistaken. Defendants nowhere disclosed—in their list of "risk factors" or elsewhere—that the Company did not adhere to the cybersecurity practices detailed in the Security Statement. Just the opposite, the Security Statement remained unchanged and prominently posted on the Company's website throughout the Class Period. And the law is clear that "risk factors" do not insulate Defendants from liability for misrepresentations about a company's actual practices. *See, e.g.*, *Lormand*, 565 F.3d at 245, 247 (risk warning that the company's business "may suffer" irrelevant where defendants made misstatements about its actual practices); *Jaroslawicz v. M&T Bank Corp.*, 962 F.3d 701, 713-14 (3d Cir. 2020) (risk warning that company faced "compliance and legal risk" from "noncompliance with laws, rules, [and] regulations" irrelevant where company "omitted company-specific detail about its compliance program"); *see also In re Barrick Gold Sec. Litig.*, 2015 WL 1514597, at *13 (S.D.N.Y. Apr. 1, 2015) ("warn[ing] of the risk of the specific litigation that resulted in [investor loss]" irrelevant when "defendants' alleged misstatements regarding … compliance meant that investors could not accurately weigh that risk").

Nothing in Defendants' cited cases remotely supports their novel contention that a company is free to lie about its cybersecurity practices so long as it includes a "risk warning" of a possible future cyberattack. To the contrary, Defendants' authorities cited throughout their brief make clear that statements—such as those contained in the Security Statement—are actionable.

For example, Defendants primarily attempt to rely upon *In re Marriott International, Inc., Customer Data Security Breach Litigation*, 2021 WL 2407518 (D. Md. June 11, 2021) ("*Marriott*"). But in *Marriott*, the court specifically stressed that—unlike in this case—none of the statements at issue were of a "character that could be proven true or false." *Id*. at *27. Furthermore, the *Marriott* court approvingly cited to *Equifax*, in which the court ***denied*** a motion

to dismiss a complaint that involved many statements similar to those at issue here. *Id*. The *Marriott* court agreed that the cybersecurity statements at issue in *Equifax* were actionable, including Equifax's statements that it "had 'strong data security and confidentiality standards' and maintained 'a highly sophisticated data information network that includes advanced security, protections and redundancies.'" *Id*. As the *Marriott* court explained, the statements at issue in *Equifax* "[we]re of a character that could be proven true or false and cross the line from puffery into material statement." *Id*. In granting defendants' motion to dismiss, the *Marriott* court emphasized that, "unlike the statements found to be actionable in *Equifax*, Marriott made no characterization at all with respect to the quality of its cybersecurity, only that Marriott considered it important." *Id*. Here, just like in *Equifax* (and unlike in *Marriott*), SolarWinds made repeated misstatements in the Security Statement and elsewhere describing and characterizing its purported cybersecurity controls.

Defendants also mistakenly try to rely upon *In re Heartland Payment Systems, Inc. Securities Litigation*, 2009 WL 4798148 (D.N.J. Dec. 7, 2009) ("*Heartland*"). But, unlike here, the *Heartland* plaintiffs neglected to plead any evidence that the defendants failed to adhere to their stated cybersecurity commitments. *Id*. For this same reason, the *Equifax* court found that *Heartland* "is distinguishable." *Equifax*, 357 F. Supp. 3d at 1220. In *Heartland*, plaintiffs attempted to show falsity merely by alleging that Heartland "suffered a security breach." *Id* at 1221. The *Equifax* court, in denying defendants' motion to dismiss and distinguishing *Heartland*, explained that the Equifax plaintiff (unlike in *Heartland*) "has not alleged that the Defendants' statements concerning Equifax's cybersecurity practices are false merely because Equifax suffered a security breach. Instead, the Plaintiff has asserted specific factual allegations describing the poor state of Equifax's cybersecurity." *Id*. Here, just like in *Equifax* (and unlike in *Heartland*), the

Complaint demonstrates through 11 witness accounts and other detailed allegations that SolarWinds lacked the cybersecurity controls specified in its Security Statement. *Id*. at 1219 ("Given the dangerously deficient state of Equifax's cybersecurity, the Court concludes it was false, or at least misleading, for Equifax to tout its advanced cybersecurity protections.").

In their reply brief, Defendants may also attempt to rely upon *In Re First American Financial Corp. Securities Litigation*, No. 2:20-cv-09781-DSF-E (ECF No. 67) (C.D. Cal. Sept. 22, 2021) ("*First American*"). But that decision—just like *Marriott* and *Heartland*—is easily distinguished. In *First American*, defendants made only vague statements that they were "committed" to cybersecurity and "serious" about cybersecurity. *Id*. In stark contrast, here, SolarWinds made specific representations in its Security Statement and elsewhere that particular cybersecurity practices and protocols were in place at the Company, *e.g.*, security training for all employees, a password policy with particular requirements including that passwords be individually salted and hashed, and segmentation of networks. Simply put, nothing in *First American* or any of the cases Defendants cite permits a corporation to tell investors that it has cybersecurity controls that it lacks.

Third, Defendants assert (Mot. at 5, 18) that, as a factual matter, the Complaint is wrong, and that SolarWinds did have a dedicated "security team" after all. But Defendants' self-serving "factual background" is not credible and, more relevant here, cannot be accepted at this stage. Tellingly, the primary "basis" for Defendants' factual assertion is a challenged misstatement ***by Defendant Brown*** himself repeating the misrepresentation that the Company had a "security team." *See* Mot. at 5, 34 n.35 (citing Biles Decl. Ex. 8). And the additional "support" for Defendants' factual assertion that there was a security team is a press release announcing the hiring of Rani Johnson—an employee who had absolutely no responsibility for security whatsoever. *See*

Mot. at 33-34. The press release announcing her hiring—which Defendants impermissibly attach to their motion—makes no mention of "security" or a "security team," but instead describes Ms. Johnson's role as focusing on "sales and product management." Biles Decl. Ex. 9.

Equally baseless is Defendants' assertion (Mot. at 18) that the Complaint is somehow "self-defeating" because SolarWinds had one employee responsible for cybersecurity—first Thornton-Trump and, after his resignation, Defendant Brown. It is Defendants' argument that is self-defeating. By definition, one person is not a "team," and as Thornton-Trump made abundantly clear in his Presentation, SolarWinds needed dedicated security employees and executives alike to carry out the reforms that were so desperately needed. There was no "security team" at SolarWinds, and Defendants' attempt to manufacture one at the pleading stage fails.

Fourth, Defendants incorrectly claim (Mot. at 34) that "[n]one of the [former employees'] statements refute the Security Statement." The 11 former SolarWinds' employees discussed in the Complaint describe in detail how the specific security practices, policies, and training identified in the Security Statement did not exist at SolarWinds. These accounts, which are corroborated by reports from the *New York Times* and myriad other facts in the Complaint, readily satisfy the pleading standards. *See In re Daou Sys., Inc.*, 411 F.3d 1006, 1021 (9th Cir. 2005) (falsity established because "[p]laintiffs provide several accounts of confidential witnesses claiming that [training program] did not in fact exist").

Also without merit is Defendants' related assertion (Mot. at 34) that the former employees cited in the Complaint were not "in positions to know anything" about "SolarWinds' cybersecurity infrastructure." To start, Thornton-Trump specializes in cybersecurity, was the Global Cybersecurity Lead at SolarWinds in advance of the Class Period, and conducted an analysis of the Company's cybersecurity deficiencies prior to his Presentation to the Company's top

executives. The other ten employees cited in the Complaint include professionals from throughout the organization and include, among others, a security specialist (FE 3), a security account manager (FE 8), an engineer (FE 9), and human resource personnel responsible for on-boarding employees, including providing them with any policies and training (FEs 5 and 6). While Defendants try to fault Lead Plaintiff for not citing former employees who were members of SolarWinds' security team, their attack misses the mark for an obvious reason: ***SolarWinds did not have a security team***.

In accordance with Fifth Circuit law, the Complaint identifies the former employees' dates of employment, positions in the company, and basic job descriptions. *See* ¶¶84 n.21, 91 n.22, 92 n.23, 93 n.24, 94 n.25, 97 n.26, 98 n.27, 99 n.28-29, 100 n.30, 101 n.31. Nothing more is required at this stage. *See Rougier v. Applied Optoelectronics, Inc*, 2019 WL 6111516, at *11 (S.D. Tex. Mar. 27, 2019) ("The Fifth Circuit ... allows a plaintiff to use confidential sources as long as those sources are described 'with sufficient particularity to support the probability that a person in the position occupied by the source would possess the information pleaded.'").

Fifth, Defendants fare no better when they assert *ipse dixit* (Mot. at 17-18, 35) that the Company reformed and began adhering to the Security Statement after Thornton-Trump resigned. The Complaint includes a plethora of facts that demonstrate the opposite, including (i) the accounts of the ten other witnesses cited in the Complaint, each of whom worked at SolarWinds for years during the Class Period and describe how the Company continued to lack the represented cybersecurity controls; (ii) investigative reports by the *New York Times*, *Reuters*, and other major media outlets confirming that the cybersecurity deficiencies persisted during the Class Period; (iii) the undeniable fact that the Company's password for its critical Update Server ("solarwinds123") remained the same and publicly available throughout the bulk of the Class

Period; and (iv) SolarWinds' effective admissions, through its "Secure-by-Design" initiative, that it lacked the security team, password policies, and cybersecurity practices that it long claimed.

Defendants nevertheless urge the Court to ignore the detailed investigative reports issued by reputable media outlets, including the *New York Times*, *Bloomberg*, and *Reuters*. As Judge Atlas explained in rejecting a similar tactic, "the content of [Plaintiff's cited] articles is properly alleged" and defendants' challenges to "the accuracy of the articles is not a proper subject for a motion to dismiss." *In re Cobalt Int'l Energy, Inc.*, 2016 WL 215476, at *4 (S.D. Tex. Jan. 19, 2016). Ultimately, Defendants' alternate version of reality, in which they remedied their cybersecurity deficiencies the minute Thornton-Trump resigned, cannot be squared with the facts and, in any event, cannot be accepted as a matter of law at the pleading stage.

Moreover, Thornton-Trump's observations from before the Class Period are plainly probative of falsity. On this point, *In re BofI Holding Securities Litigation* is instructive. There, plaintiffs alleged that a former employee's pre-class period allegations regarding a company's "understaffing" supported the falsity of defendants' statements to investors during the class period eleven months later. 2017 WL 2257980, at *11 (S.D. Cal. May 23, 2017). The defendants argued, as Defendants do here, that the court should disregard the former employee's account because it was possible that the "understaffing" that he observed prior to the class period ended before the class period. *Id.* The court rejected this "temporal nexus" argument, explaining that "while it is true that Lead Plaintiff has not demonstrated … whether [the understaffing] remained … until [the end of the class period]," plaintiff is entitled to the "reasonable inference that no changes had been made in the interim and that [BofI] remained understaffed during the quarters that were the subject of [defendant's] statements" to investors. *Id.* As the court explained, "[t]he PSLRA and Rule 9(b) only require that Lead Plaintiff provide particularized reasons why a statement was false or

misleading at the time it was made, not that Lead Plaintiff prove its entire case in the complaint and without the benefit of reasonable inferences." *Id.* at *12.

As in *BofI*, there is no reason to believe that the cybersecurity deficiencies identified by Thornton-Trump were remediated upon his departure and before the Class Period. And there are myriad reasons to conclude they were not, including the accounts of ten former SolarWinds' employees, numerous investigative reports, the fact that SolarWinds used a compromised password for its critical Update Server for one-and-a-half years and during the bulk of the Class Period, and the fact that the Company has admitted, through its "Secure-by-Design" initiative, that it lacked basic cybersecurity protections during the Class Period. Particularly on these facts, Lead Plaintiff is entitled to the "reasonable inference that no changes [were] made in the interim" between Thornton-Trump's departure and the start of the Class Period. *BofI*, 2017 WL 2257980, at *11; *see also Transocean Ltd.*, 866 F. Supp. 2d at 241("[G]iven that all facts in the Complaint are taken as true and all reasonable inferences are drawn in Plaintiffs' favor at this stage—it is reasonable to infer that the practices were in place at the time of the Proxy.").

Sixth, Defendants assert that "there is no link between any challenged statement and the Cyberattack." (Mot. at 35). Defendants' argument conflates the "falsity" and "loss causation" inquiry. "Falsity" and "loss causation" are two distinct elements of a securities law claim. It is "loss causation," not "falsity," that concerns the "causal link" between the alleged misconduct and the resulting harm suffered by the plaintiff. *See Huddleston v. Herman & MacLean*, 640 F.2d 534, 549 n.24 (5th Cir. 1981) ("'[L]oss causation' refers to a direct causal link between the misstatement and the claimant's economic loss."). And, in the Fifth Circuit, loss causation is subject to the liberal Rule 8 pleading standard, which only "requires the plaintiff to allege a facially 'plausible' causal relationship between the fraudulent statements or omissions and plaintiff's economic

loss." *Lormand*, 565 F.3d at 258. Lead Plaintiff has easily satisfied this requirement, as further discussed below at pages 64-67 (Section III.C).

In any event, Defendants are wrong. The fact of the matter is that SolarWinds had severely deficient security, and it got hacked as a result. ¶¶150, 152, 154, 156-163. Defendants' contention that Lead Plaintiff must go much farther and do the impossible at the pleading stage—definitively prove, without any discovery, precisely how the Company's cybersecurity deficiencies and compromised Update Server password caused the cyberbreach—finds no support in the law. *See In re BHP Billiton Ltd. Sec. Litig.*, 276 F. Supp. 3d 65, 85 (S.D.N.Y. 2017) (rejecting defendants' argument that statement concerning the toxicity of river following a catastrophic dam collapse was not false because the complaint failed to set forth "that toxins were introduced into the Rio Doce"). As courts in this Circuit have repeatedly explained in denying motions to dismiss Exchange Act claims, "the particularity rules should not be interpreted to require the pleading of facts which, because of the lack of discovery, are in defendants' exclusive possession." *In re Fleming Cos. Inc. Sec. & Derivative Litig.*, 2004 WL 5278716, at *6 (E.D. Tex. June 16, 2004). "A securities fraud plaintiff need not allege all facts that may be related to his claims…." *Id.* "[S]uch a requirement is impossible at the pleading stage because usually only the defendants know all the facts related to the alleged fraud." *Id*.

Not surprisingly, none of Defendants' cited authorities conflate "falsity" and "loss causation." For example, *Izadjoo v. Helix Energy Sols. Grp., Inc.*, 237 F. Supp. 3d 492 (S.D. Tex. 2017), relied upon by Defendants in support of their novel contention, did not even discuss—much less require—a "link" between the alleged misconduct and an adverse event; rather, there, the court faulted the plaintiff for failing to "link" a former employee's observations of misconduct and alleged false statements at issue in the case. *Id*. at 511. Here, there is no question that the accounts

of Ian Thornton-Trump and the ten former employees are "linked" to the misstatements in the Security Statement—they each detail how the core cybersecurity controls listed in the Security Statement did not exist at SolarWinds.[2]

Seventh, Defendants argue that they cannot be held responsible for their misrepresentations because the Security Statement was not an "investor-directed communication." *See* Mot. at 33. Defendants' argument is factually incorrect and finds no legal support. To be actionable, the alleged misrepresentation need only be public, which website statements unquestionably are. Moreover, investors rely upon statements on companies' official websites all the time, and courts routinely hold companies liable for misrepresentations on their websites. *See, e.g.*, *Howard v. Arconic Inc.*, 2021 WL 2561895, at *14 (W.D. Pa. June 23, 2021) ("[I]t is certainly plausible that any rational seller of securities would operate on the belief that investors would visit the Company's website."); *Equifax*, 357 F. Supp. 3d at 1227 (sustaining securities fraud claims based on false statements concerning cybersecurity made on company's website); *Jackson Cnty. Emps.' Ret. Sys. v. Ghosn*, 510 F. Supp. 3d 583, 606 (M.D. Tenn. 2020) (same); *S.E.C. v. Enterprises. Sols., Inc.*, 142 F. Supp. 2d 561, 577-78 (S.D.N.Y. 2001) (same); *see also In re Volkswagen "Clean Diesel" Mktg., Sales Pracs., & Prod. Liab. Litig.*, 2017 WL 66281, at *18 (N.D. Cal. Jan. 4, 2017) (rejecting defense that emission compliance stickers on diesel Volkswagens were "directed toward consumers and not the investing public," and declining to "declare as a matter of law that a reasonable investor would not have considered the emissions stickers on Volkswagen Vehicles to be material investing information"). Such a result is particularly warranted here because the

[2] And, unlike in *In re BP p.l.c. Securities Litigation*, SolarWinds' cost-cutting occurred before the cyberbreach—not afterwards. *See* 852 F. Supp. 2d 767, 795 (S.D. Tex. 2012). (finding allegations illogical because the oil spill occurred "at least a year before any of the alleged cost-cutting measures occurred").

Security Statement was linked to every page of SolarWinds' website, including those exclusively for investors. ¶¶37, 186.

Defendants' cases do not remotely suggest that a company cannot be held liable for misstatements on their website, much less for statements contained in an official document such as SolarWinds' Security Statement. Tellingly, the lone case that Defendants cite in support of their novel contention—*SEC v. Tex. Gulf Sulphur Co.*, 401 F.2d 833 (2d Cir. 1968)—was decided before the advent of the Internet. As courts have explained in rejecting Defendants' precise argument here, "whether a reasonable investor would have utilized the website for such information [] would necessarily involve considerations of fact which is wholly inappropriate at this stage of the litigation." *In re Massey Energy Co. Sec. Litig.*, 883 F. Supp. 2d 597, 617 (S.D. W. Va. 2012).

Finally, Defendants erroneously attempt to escape liability by contending that they did not author the Security Statement. *See* Mot. at 37; Thompson Mot. at 37 (citing *Janus Cap. Grp., Inc. v. First Derivative Traders*, 564 U.S. 135 (2011) ("*Janus*")). But, as the Supreme Court made clear in *Janus*, the securities laws impose liability on corporate executives who have "ultimate authority over the statement," regardless of whether they wrote the statement. *Id*. at 142. Even when a corporate executive "did not sign any of the [statements] at issue, he still may be found to have made a misstatement" under *Janus*. *In re Fannie Mae 2008 Sec. Litig*., 891 F. Supp. 2d 458, 473 (S.D.N.Y. 2012). Indeed, "in the post-*Janus* world, an executive may be held accountable where the executive had ultimate authority over the company's statement; signed the company's statement; ratified and approved the company's statement; ***or*** where the statement is attributed to the executive." *Id*.

Here, Defendants Brown and Thompson had "ultimate authority" over the Security Statement. The Complaint details how: (i) Defendants Brown and Thompson "reviewed and approved" the Security Statement (¶37); (ii) Defendant Brown publicly affirmed that he was "responsible for the security of [SolarWinds'] products ... as well as the security for [SolarWinds'] infrastructure" (¶188); (iii) Defendant Brown repeatedly directed investors and the public to the Company's Security Statement and publicly stressed that companies, like SolarWinds, "publish their security protocols and processes so you can evaluate whether they meet your standards" (¶186); (iv) Defendant Brown was the face—literally—of the Security Statement, with his picture plastered on the cover of the Security Center that housed the Security Statement (¶188); and (v) Defendant Brown confirmed his authority and ownership of the Security Statement by, among other things, welcoming investors and the public to "***our*** new security resource center" (*id.*).

The Complaint's allegations more than suffice to demonstrate that Defendants Brown and Thompson had "ultimate authority" over, and thus are properly deemed "makers" of, the Security Statement. *See Ferris v. Wynn Resorts Ltd.*, 2021 WL 3216462, at *13 (D. Nev. July 28, 2021) (corporate executives deemed "makers" of the statement where complaint "alleges that these defendants were among the Company's most senior executives, were involved in the Company's day-to-day affairs, and 'were provided with copies of the [statement for approval]'"); *In re Rocket Fuel, Inc. Sec. Litig.*, 2015 WL 9311921, at *10 (N.D. Cal. Dec. 23, 2015) (insider defendants deemed "makers" of the website statement because the complaint alleged they "'possessed the power and authority to control the contents of the Company's press releases [and] investor and media presentations'"); *In re Pfizer Inc. Sec. Litig.*, 2012 WL 983548, at *4 (S.D.N.Y. Mar. 22, 2012) ("Given the allegations that the Individual Defendants 'approved or ratified' any statements issued by Pfizer, the [complaint] adequately pleads that such statements were attributed to and

ultimately controlled by the Individual Defendants."); *see also In re Puda Coal Sec. Inc., Litig.*, 30 F. Supp. 3d 261, 267 (S.D.N.Y. 2014) (underwriters found to have "made" statement in part because "[t]he front cover of the prospectus prominently displayed [their] names, thus endorsing the statements").

Defendants' arguments to the contrary, at the very most, raise factual disputes unfit for resolution at this stage. *See, e.g.*, *T. Rowe Price Growth Stock Fund, Inc. v. Valeant Pharms. Int'l, Inc.*, 2018 WL 395730, at *5 (D.N.J. Jan. 12, 2018) (argument that false statements cannot be attributed to executive defendant was "better suited for adjudication at a later stage"); *see also Moon Joo Yu v. Premiere Power LLC*, 2018 WL 456244, at *10 (S.D.N.Y. Jan. 17, 2018) ("[C]ourts have consistently found that multiple persons can be considered to have made a statement.").

On this point, Defendants' cited cases are easily distinguishable. Unlike in *Janus*, Lead Plaintiff does not seek to hold a "separate legal entity" responsible for SolarWinds' Security Statement (*Janus*, 564 U.S. at 138); rather, Lead Plaintiff seeks to hold responsible the Company's top executives with "ultimate authority" over the statements. *See In re Pfizer Inc. Sec. Litig.*, 936 F. Supp. 2d 252, 268-69 (S.D.N.Y. 2013) ("*Janus* 'addressed only whether third parties can be held liable for statements made by their clients ... and has no bearing on how corporate officers who work together in the same entity can be held jointly responsible on a theory of primary liability.'"). And, unlike in *Southland Securities Corporation v. INSpire Insurance Solutions, Inc.*, the Complaint ***does*** "specify which … document[] is attributable" to each defendant. 365 F.3d 353, 365 (5th Cir. 2004). Likewise, in contrast to *Plaisance v. Schiller*, 2019 WL 1205628 (S.D. Tex. Mar. 14, 2019), the Complaint's attribution of the Security Statement to the Defendants is

not "based solely on [the defendants] title[s]," but rather detailed allegations demonstrating their approval and ownership of the Security Statement. *Id*. at *16.

In any event, it is inarguable—and Defendants do not contest—that, at minimum, Defendant SolarWinds is properly deemed a "maker" of its Security Statement. *See Rocket Fuel*, 2015 WL 9311921, at *10 ("[P]laintiffs may also attribute the [website] statement to the company itself, which is also named as a defendant on the Exchange Act claims."). It is equally beyond dispute that, in evaluating SolarWinds' liability in the Fifth Circuit, the Court looks not only to the mental state of the person who authored the Security Statement, but also the executives who "'approve[d] it or its making or issuance, or who furnish[ed] information or language for inclusion therein, or the like.'" *See Lee v. Active Power Inc.*, 29 F. Supp. 3d 876, 884-85 (W.D. Tex. 2014) ("[T]he Court rejects Defendants' view that [an individual defendant's] scienter cannot be imputed to [the company] because [the defendant] did not 'make' the alleged false statements … as this is not a legal requirement under *Southland*.").

2. Defendants Misleadingly Touted The Company's Cybersecurity Controls, Omitting Material Facts That Undermined Their Statements

In addition to their misstatements in the Security Statement, Defendants also repeatedly touted SolarWinds' cybersecurity controls in their public statements without disclosing that—in truth—they had no such controls. In so doing, they violated the basic disclosure principle that, once a corporate executive speaks on a subject, he "has a duty to tell the whole truth, and disclose 'material, firm-specific adverse facts that affect the validity or plausibility' of his statement." *In re ArthroCare Corp. Sec. Litig.*, 726 F. Supp. 2d 696, 716 (W.D. Tex. 2010); *see also Kurtzman v. Compaq Comput. Corp.*, 2000 WL 34292632, at *22 (S.D. Tex. Dec. 12, 2000) (because the defendants "voluntarily chose to speak publicly" on a topic, they "therefore had a duty to tell the whole truth").

For example, Defendant Brown stressed during Class Period interviews that "[w]e are making sure that there is good basic hygiene" at SolarWinds (¶222) and that "one of the things that we've focused on, that my team focuses on, is on heavy-duty hygiene" (¶220). Defendants further represented that SolarWinds "appl[ied] appropriate administrative, operational, and technical security controls to help ensure that our customer data is handled and processed in a responsible and secure manner," emphasizing that customers' "security and privacy are our top priorities at SolarWinds." ¶¶216, 218.

In making these and the other representations detailed in the Complaint, Defendants were duty bound—but failed—to disclose that SolarWinds lacked basic security practices, procedures, and policies. They had no security team (¶¶95, 115), no information security policy (¶118), provided no security training to employees (¶¶126-30), lacked any password policy (¶¶119, 122), failed to segment the network or limit user authorization (¶¶91, 101, 133-35), and did not perform background checks on employees (¶¶96-97, 138-39).

Courts across the country hold that statements that tout the strength, quality, or character of an aspect of a business—such as Defendants' statements touting their "cybersecurity" controls—are actionable where, as here, they misstate or omit material facts. For, instance, an airline's statements touting its safety record and assuring investors that its "paramount goal was profitability while maintaining operational integrity" were misleading and actionable when the company's maintenance practices were, in reality, woefully deficient. *In re ValuJet, Inc.*, 984 F. Supp. 1472, 1477 (N.D. Ga. 1997). A mining company's statements that "[w]e have a comprehensive range of measures in place to protect [environmental] areas and resources," were misleading and actionable when it lacked such measures. *Barrick Gold*, 2015 WL 1514597, at *4, 11-12. Another mining company's statements touting its commitment to safety, including that

"we make [safety] a priority every day" were misleading and actionable when safety was not a priority. *See Massey Energy*, 883 F. Supp. 2d at 614. SolarWinds' misleading statements were of the same type; they concerned a critical business practice (cybersecurity) of central import to customers and investors alike and omitted material information.

Defendants try to recast their statements as "immaterial puffery"—i.e., corporate fluff. Their attempt fails. Only statements that "contain no concrete factual or material misrepresentation" may be deemed "puffery." *Lormand*, 565 F.3d at 249 n.14. Determining whether a statement is "material" involves "a mixed question of law and fact [that] it is usually left for the jury." *Fener v. Belo Corp*., 513 F. Supp. 2d 733, 746 (N.D. Tex. 2007). "The Court will not dismiss a complaint on grounds of immateriality of the alleged misrepresentation unless the misrepresentation is 'so obviously unimportant to a reasonable investor that reasonable minds could not differ on the question of their importance.'" *McNamara v. Bre-X Mins. Ltd.*, 197 F. Supp. 2d 622, 685 (E.D. Tex. 2001). Defendants have not—and cannot—make such a showing here.

Defendants' misrepresentations concerned a core aspect of their business that they publicly described (albeit falsely) as one of their "top priorities." ¶¶140, 186. Having done so, they cannot now credibly claim that their statements about cybersecurity were "obviously unimportant." As the *Equifax* court explained in rejecting a similar argument, "the Court cannot say, as a matter of law, that Equifax's representations that its cybersecurity efforts were extensive or that it was 'committed' to data security were so 'obviously un-important' to its shareholders that they should be considered immaterial." *See Equifax*, 357 F. Supp. 3d at 1224.

The context of Defendants' statements further undermines their "puffery" contentions. Cybersecurity was critical to SolarWinds' ability to win business. For this reason, Defendant

Brown and SolarWinds specifically portrayed themselves as experts in cybersecurity and SolarWinds as the go-to company to ensure that customer data was safely handled. They stressed over-and-over the importance of cybersecurity, and reassured investors time-and-again that they were singularly focused on it. *See* ¶¶36, 39. Particularly in this context, Defendants' statements touting their cybersecurity controls—which were, in truth, totally absent—cannot be cast aside, as a matter of law, as mere "puffery." *See Rougier*, 2019 WL 6111516, at *10 (statements not puffery where plaintiffs "alleged specific facts to show that Defendants' statements were belied by" circumstances at the time). And, in any event, "[e]ven if these statements were looked upon as mere 'puffery,' as the defense claims, that does not negate the duty to disclose other information necessary to make those statements not misleading." *Marcus v. J.C. Penney Co., Inc.*, 2015 WL 5766870, at *5 (E.D. Tex. Sept. 29, 2015).

Defendants' cited cases are distinguishable. In *In re Extreme Networks, Inc. Securities Litigation,* the defendants "committed" to a result that that could only be achieved in the future. 2018 WL 1411129, at *23 (N.D. Cal. Mar. 21, 2018). In contrast, SolarWinds made statements touting its ***current*** cybersecurity controls. Likewise, in *Marriott*, the defendant "in no way certif[ied] that it used particular methods to secure data," and the hotel company's "core business" did not involve security. 2021 WL 2407518, at *27. Here, in contrast, SolarWinds ***did*** certify that "it used particular methods to secure data," and its statements ***did*** concern a "core aspect of [its] business." Finally, in *In re Alphabet, Inc. Securities Litigation*, defendants did not make statements describing their steps to secure customers' privacy, but instead made only "generalized statements regarding the importance of privacy." 2020 WL 2564635, at *4 (N.D. Cal. Feb. 5, 2020), *aff'd in part, rev'd in part and remanded*, 1 F.4th 687 (9th Cir. 2021). Here, Defendants made misrepresentations that went well beyond "generalized statements regarding the importance"

of cybersecurity; they represented (falsely) that SolarWinds took specific steps to safeguard cybersecurity.

Defendants also attempt to characterize their statements as mere "opinions." Mot. at 36-37. Defendants' statements were not opinions. For example, Defendant Brown's statement that "one of the things that we've focused on, that my team focuses on, is on heavy-duty hygiene" (¶220) is a statement of fact. Similarly, SolarWinds' statement that the Company "makes sure everything is backed by sound security processes, procedures, and standards" (¶36) is one of fact. As the *Equifax* court explained in rejecting a similar challenge, statements that "Equifax employs strong data security and confidentiality standards" and "maintain[s] a highly sophisticated data information network that includes advanced security, protections and redundancies … do not constitute … subjective opinion[s]." 357 F. Supp. 3d at 1231. Defendants' statements contained no language indicating that the speaker was opining on anything, but, rather, were statements of what Defendants and SolarWinds were purportedly doing.

In any event, even if Defendants' statements could be characterized as "opinions," they would still be actionable. In the Fifth Circuit, "[i]f the underlying facts are not provided and contradict the opinion statement, the statement will be misleading by omission and the speaker can be held liable." *Ramirez v. Exxon Mobil Corp.*, 334 F. Supp. 3d 832, 848 (N.D. Tex. 2018). Here, Defendants' statements omitted key facts that contradicted their statements—namely, that they followed ***none*** of the basic security practices that they represented to investors. *See supra* at § III.A.1. These omissions render their statements actionable, even if now rewritten as "opinions."

B. The Complaint Pleads A Strong Inference Of Scienter

A party satisfies the scienter pleading requirement by alleging ***either*** an "intent to deceive" ***or*** "severe recklessness." *Spitzberg*, 758 F.3d at 684; *ArthroCare Corp.*, 726 F. Supp. 2d. at 711. An inference of scienter need not be "irrefutable, i.e., of the 'smoking-gun' genre, or even 'the

most plausible of competing inferences.'" *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 324 (2007). Rather, a complaint's scienter allegations suffice even when reasonable, non-culpable inferences exist, and without allegations of motive. *Id*. at 325. In assessing scienter, the "inquiry is whether all of the facts alleged, taken collectively, give rise to a strong plausible inference of scienter, not whether any individual allegation, scrutinized in isolation, meets that standard." *Lormand*, 565 F.3d at 251. A complaint cannot be dismissed if "a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs*, 551 U.S. at 324. Stated differently, "a tie favors the plaintiff." *Spitzberg*, 758 F.3d at 686.

Severe recklessness does ***not*** require that Defendants know that their statements are false. *Id*. As the Fifth Circuit has explained, whether "[defendants] actually believed [their statements to be true] ***is irrelevant*** to whether [defendants] were severely reckless." *Id*. And a "strong inference of fraud may be established where the complaint sufficiently alleges that the defendants … failed to check information they had a duty to monitor." *Fleming*, 2004 WL 5278716, at *10.

1. The Complaint Adequately Alleges A Strong Inference Of Scienter As To Defendant Brown

a. Defendant Brown Held Himself Out As "Responsible" For Cybersecurity At SolarWinds

Defendant Brown's self-proclaimed knowledge and ownership of the "cybersecurity controls" at SolarWinds supports a strong inference that he knew, or was severely reckless in failing to know, that the Company lacked such controls. Defendant Brown was the only person responsible for cybersecurity at SolarWinds. He publicly emphasized that he was ***"responsible for the security of [SolarWinds'] products ... as well as security for [its] infrastructure."*** ¶16. Additionally, Brown was the face of SolarWinds' "cybersecurity"—with his image and a video of him prominently featured on the top portion of the Security Center, housing the Security

Statement. ¶38. Defendant Brown did interviews on podcasts and with popular IT publications during the Class Period, professing the importance of and his deep knowledge about the specific cybersecurity controls that, unknown to investors, SolarWinds lacked. *See* ¶¶36, 40, 220, 222.

That Defendant Brown presented himself as the hands-on leader of SolarWinds' cybersecurity supports a strong inference of his scienter. In *BP*, for example, the court found a strong inference of scienter as to the defendant chief executive officer because his "own actions as the spokesperson and champion for BP's reform efforts weigh[ed] strongly in favor of the inference that [he] paid special attention to BP's process safety efforts or, at the least, was reckless in not doing so while continuing to publicly tout improvements." 843 F. Supp. 2d at 783. As the court explained, "the competing inference—that [the BP executive] professed to be focused on process safety but remained unaware of [the] actual … concerns in BP's operations on the ground—is far less compelling." *Id*.

So too here. Defendant Brown presented himself—repeatedly—as the spokesperson and champion of cybersecurity at SolarWinds, which strongly supports an inference of his scienter and defeats any competing inference that he lacked knowledge about this critical subject in which he specialized and frequently discussed in public. Defendants make no attempt to argue that Defendant Brown could reasonably have been unaware of the true state of cybersecurity at SolarWinds. And it defies credulity to believe that he did not know that, contrary to his and the Company's statements, SolarWinds lacked a security team, did not conduct cybersecurity training, did not have a password policy, did not segment its networks, and did not conduct security background checks on new employees. *See* ¶¶113-49.

For this reason alone, Defendants' cited authorities (including *Heartland* and *Marriott*) are easily distinguished. The defendants in those cases were general corporate executives without any

responsibility for security. In contrast, Brown was the only person responsible for cybersecurity, a self-proclaimed expert in the field, identified himself as "responsible" for SolarWinds' cybersecurity, and spoke extensively about the very practices SolarWinds lacked—all while directing investors and the public to his "Security Center" and its "Security Statement."

b. Defendant Brown Knew About The Failure Of The Password Policy And "solarwinds123"

The scienter inference is further strengthened by the fact that Defendant Brown and SolarWinds learned no later than November 19, 2019 (i.e., mid-way through the Class Period), that the Company's internal password to its critical Update Server was "solarwinds123," and this key password was publicly available on a popular public website for approximately one-and-a-half years. ¶¶105-12, 185. In addition to being the password to the Company's critical Update Server, "solarwinds123" was also the default password used throughout the Company to access a variety of sensitive data. ¶¶99, 122-23.

Upon learning of this egregious cybersecurity failure, Defendant Brown was obligated to check—if he somehow did not already know—whether the Company had a password policy (it did not), required "individual[ized]" passwords (it did not), provided employees cybersecurity training (it did not), and otherwise followed the Security Statement (it did not). Of course, as a purported cybersecurity expert such as Defendant Brown would know, SolarWinds' egregious compromise of its Update Server password would not have been possible had the Company in fact had a password policy or required individualized passwords. On these facts, "[t]he only compelling, possible inference is that [Brown and SolarWinds] were either aware of the truth and intentionally misled investors ... or were willfully blind and severely reckless in ignoring the truth." *ArthroCare*, 726 F. Supp. 2d at 718. As the Fifth Circuit has recognized, "an egregious refusal to

see the obvious, or to investigate the doubtful, may … give rise to an inference of recklessness." *Plotkin*, 407 F.3d at 700 (citing *Novak v. Kasaks*, 216 F.3d 300, 308 (2d Cir. 2000)).

Faced with these well-pled allegations, Defendants argue that the November 2019 email alerting Brown and SolarWinds to the multi-year compromise of the Update Server does not strengthen the scienter inference because "all of the challenged statements were made" before their receipt of the email. Mot. at 24. This is incorrect. SolarWinds continuously—on each day during the Class Period—published the Security Statement unchanged. *See* ¶201 (Security Statement maintained on the SolarWinds website "[t]hroughout the Class Period…"). In fact, after being informed that the Update Server had been compromised for a year-and-a-half, Defendant Brown ***continued*** to direct investors and the public to his Security Statement, including in his September 10, 2020 article discussing "security statements" and during an October 13, 2020 podcast episode. ¶¶39 & n.4, 40; *see also Ghosn*, 510 F. Supp. 3d at 595 (finding scienter inference pled where misstatements on website were "published … throughout the Class Period").

Defendants next seek to minimize the fact that the Company's critical Update Server was compromised for one-and-a-half years by noting that the password ("solarwinds123") was set by an "intern." Mot. at 23, 25. Their effort fails. That SolarWinds gave an intern access to its critical Update Server and—worse yet—entrusted the intern with the power to set the internal password for the Update Server, were blatant violations of the Security Statement as well as further evidence that a password policy never existed at SolarWinds.

Equally baseless is Defendants' factual contention that the "solarwinds123" password was not the cause of the cyber breach. Mot. at 23. In support of this factual assertion, Defendants assert that the Update Server is maintained by a third-party and is only used to download non-Orion software. But this self-serving assertion—like so many in SolarWinds' brief—cannot be

accepted as a matter of law at this stage. As courts in this District and elsewhere have repeatedly explained in rejecting this tactic, "the strong-inference pleading standard does not license the court to resolve disputed facts at this stage in the case." *City of Pontiac Gen. Emps.' Ret. Sys. v. Dell Inc.*, 2016 WL 6075540, at *4 (W.D. Tex. Sept. 16, 2016); *BP*, 843 F. Supp. 2d at 767 n.21. Moreover, even assuming the compromised Update Server was not the source of the cyberattack, it surely strengthens the scienter inference that Brown and SolarWinds (i) learned of this dangerous, long-standing violation of the Security Statement, which exposed its customers to the precise cyberbreach that SolarWinds ultimately experienced; and (ii) did not check whether the Company maintained the cybersecurity controls identified in its Security Statement and touted elsewhere. Had Defendant Brown and SolarWinds checked, they would have learned that the Company lacked each and every one of the basic cybersecurity controls represented in the Security Statement. *See Fleming*, 2004 WL 5278716, at *10-11 (a "strong inference of fraud may be established where the complaint sufficiently alleges that the defendants … failed to check information they had a duty to monitor")

Contrary to Defendants' spin, the compromise of SolarWinds' critical Update Server was not merely a "discrete violation[] of SolarWinds' password practices." Mot. at 25. That the "solarwinds123" password was (i) set by an intern as the Update Server password, (ii) remained unchanged for two years, (iii) posted on a public website, (iv) publicly available for one-and-a-half years, and (v) also the password for other databases and systems, is not just an isolated password policy failing, but powerful evidence of SolarWinds' comprehensive failure to secure and monitor its sensitive assets and protect its customers from malicious actors. *See* ¶158. As Professor Terry Thompson of John Hopkins University correctly observed, SolarWinds' compromise of its Update Server was "an egregious violation of fundamental standards of

cybersecurity" and reflects that SolarWinds was "an organization rife with systemic security issues, an ineffective security management program, and a lack of technical controls or compliance with industry standards." ¶158.

c. Defendant Brown Paid Particular Attention To Cybersecurity Because It Was Critical To SolarWinds Customers

The scienter inference against Defendant Brown is further bolstered by the fact that cybersecurity—and specifically, the Security Statement—was an integral part of Brown's and SolarWinds' pitch to customers and investors. Brown publicly stressed that "strong vendors," such as SolarWinds, "publish their security protocols and processes so you can evaluate whether they meet your standards." ¶186. Defendant Brown and SolarWinds then directed customers—repeatedly—to the Company's Security Center and, specifically, the Security Statement. ¶¶35-42, 186. Defendant Brown and SolarWinds did this for a reason: cybersecurity was a top priority to investors and the governmental agencies that he and SolarWinds were trying to attract. ¶189.

Defendant Brown was the single-most active SolarWinds executive spreading the message that SolarWinds' security protocols and procedures qualified it to safeguard government agencies' sensitive and valuable data. ¶188. He knew how important cybersecurity was, which is why he was so dogged in promoting SolarWinds' cybersecurity prowess. Because Defendant Brown knew and spoke so regularly about the critical importance of cybersecurity to SolarWinds' customers, he knew or—at the very least—was severely reckless in failing to apprise himself of the reality that SolarWinds lacked cybersecurity. *Plotkin*, 407 F.3d at 700 (reasonable to infer defendant knew of undisclosed facts "given the importance of" the issue); *Southland*, 365 F.3d at 380 (defendant's "position as CEO" and "personal involvement in … touting" strengthened scienter inference); *Nathenson v. Zonagen Inc.*, 267 F.3d 400, 425 (5th Cir. 2001) (scienter pled where statements related to "obviously important" part of the company); *BP*, 843 F. Supp. 2d at 783

(repeated statements on topic weighed "strongly in favor of the inference that [he] paid special attention to" it "or, at the least, was reckless in not doing so").[3]

2. The Complaint Adequately Alleges A Strong Inference Of Scienter As To Defendant Thompson

The Complaint also adequately alleges that Defendant Thompson was aware of, or severely reckless in not knowing, the egregious cybersecurity deficiencies plaguing his Company. *First*, the Company's top executives, including Defendant Thompson's direct reports, attended Thornton-Trump's Presentation documenting a lack of cybersecurity controls at SolarWinds. *Second*, at Defendant Thompson's direction, the Company carried out the Private Equity Firms' cost-cutting strategy, intentionally leaving cybersecurity (a multi-million dollar per year cost) stagnant so the Company could meet analysts' quarterly earnings expectations. *Third*, Defendant Thompson's personal Class Period stock sales, suspicious in both their proximity to SolarWinds' awareness of the breach and in their dramatic departure from his pre-Class Period trading patterns, provide yet further support for the scienter inference. *Finally*, the fact that, upon Defendant Thompson's resignation, the Company's new CEO quickly recognized that the Company lacked basic cybersecurity controls further evidences that Defendant Thompson was, at minimum, severely reckless in failing to learn of these egregious deficiencies during his many years as the CEO of a Company whose stated "top priorities" supposedly included cybersecurity.

[3] Lead Plaintiff alleges far more than Brown's "status" at the Company. In any event, Defendants' own authorities recognize that "a person's status as a corporate officer, when considered alongside other allegations, can help support an inference" of scienter. *Heartland*, 2009 WL 4798148, at *7; *see also In re Triton Energy Ltd. Sec. Litig.*, 2001 WL 872019, at *10-11 (E.D. Tex. Mar. 30, 2001) (rejecting defendants' argument "that position-and-experience evidence is incompetent as proof of scienter" and explaining that "most authorities have found [the] opposite").

a. Defendant Thompson Had Actual Knowledge Of, Or Was Severely Reckless As To, Ian Thornton-Trump's Presentation

The Complaint details how Thornton-Trump (SolarWinds' Global Cybersecurity Strategist) convened a meeting of the Company's executives, which included Defendant Thompson's direct reports, Chief Technology Officer Joe Kim and Chief Marketing Officer Gerardo Dada. ¶74. The meeting was widely discussed throughout the Company. ¶84. During the meeting, Thornton-Trump conducted a formal Presentation of his findings following his months of investigation. He concluded, and told Defendant Thompson's direct reports, that SolarWinds' ***"infrastructure and corporate systems exist in a precarious state."*** ¶77. He highlighted that there was ***"No centralized reporting," "No centralized management,"*** and ***"Silos of communication."*** ¶75. In response, he was told that Defendant Thompson did not want to invest in cybersecurity and, as a result, Thornton-Trump resigned in protest. ¶¶86-87.

These allegations strengthen the scienter inference as to Defendant Thompson and SolarWinds. To start, it is implausible that neither Mr. Dada nor Mr. Kim reported Thornton-Trump's concerns to the person they immediately reported to, Defendant Thompson. This is particularly so because Mr. Dada emailed Mr. Thornton-Trump after the meeting that he ***"agree[d] with [Thornton-Trump's] assessment"*** and ***"appreciate[d] the effort and candor [he] put behind trying to do the right thing at SolarWinds."*** ¶89.

What's more, the scienter inference against Thompson is strengthened by the fact that he personally brought about the situation described by Thornton-Trump in his Presentation. ¶149. As the *New York Times* reported and witnesses recounted, under Thompson's direction, ***"common security practices were eschewed because of their expense."*** ¶147. Courts have found under similar circumstances that, "[i]f negative information [was] widely-known and discussed among the Company's senior executives, it is almost inconceivable that [a high-ranking executive] would

be unaware of the negative impact of the cost-cutting strategy that [he himself] implemented." *Hedick v. The Kraft Heinz Co.*, 2021 WL 3566602, at *12 (N.D. Ill. Aug 11, 2021) (even though executive defendant was not alleged to have been at a meeting where information contrary to public statements was relayed, that other executives attended the meetings supported an inference that executive defendant was aware of the information).

In response to the Complaint's well-pled allegations, Defendants urge the Court to ignore Thornton-Trump's Presentation. Defendants' arguments fail.

First, Defendants contend that it is possible that neither Mr. Dada nor Mr. Kim told Defendant Thompson about Thornton-Trump's Presentation. While Lead Plaintiff recognizes that anything is possible, the scienter inquiry concerns what is plausible, not possible. And it is not plausible that Mr. Dada and Mr. Kim would conceal this information from the person to whom they directly reported. Mr. Thornton-Trump's Presentation raised serious concerns, and he did not mince words, telling the executives in attendance that SolarWinds' ***"infrastructure and corporate systems exist in a precarious state."*** ¶77. Lead Plaintiff is entitled to "reasonable inferences" at this stage, and it is certainly reasonable to infer that Mr. Dada or Mr. Kim told Defendant Thompson about Thornton-Trump's findings. The inference is particularly justified here because Thompson's two reports, both of whom were top officers at the Company, agreed with Thornton-Trump's assessment. ¶¶82, 88.

Under these circumstances, Lead Plaintiff is entitled to the inference that Mr. Dada and Mr. Kim told Defendant Thompson about Mr. Thornton-Trump's alarming findings. *See Owl Creek I, L.P. v. Ocwen Fin. Corp.*, 2018 WL 4844019, *11 (S.D. Fla. Oct. 4, 2018) ("Although the Complaint does not specifically allege that Ocwen's Vice President of Compliance conveyed the backdating discovery to [executive defendant] Erbey, given Erbey's status as a high level

executive, there is a plausible inference that he was aware of the backdating scheme."); *Robb v. Fitbit Inc.*, 2017 WL 219673, at *4-6 (N.D. Cal. Jan. 19, 2017) (holistic assessment of complaint's allegations sufficiently alleged that critical company information provided to the company's COO "would also have been known to the individual defendants" even where the complaint did "not contain express allegations that [the COO] gave this information to [the other individual] defendants").

In any event, Thornton-Trump's Presentation bolsters the scienter inference ***even assuming*** Defendant Thompson's direct reports never told him about it. To establish scienter in the Fifth Circuit, Lead Plaintiff does ***not*** need to establish actual knowledge, rather "severe recklessness" is enough. *Spitzberg*, 758 F.3d at 686 (whether "[defendants] actually believed [their statements to be true] ***is irrelevant*** to whether [defendants] were severely reckless"). It would be severely reckless, at the least, for Thompson—the top officer of a Company whose "top priorities" purportedly included cybersecurity—to not check whether it had the basic cybersecurity controls represented in its Security Statement linked to every page of its website. *See Fleming*, 2004 WL 5278716, at *10-11 (a "strong inference of fraud may be established where the complaint sufficiently alleges that the defendants … failed to check information they had a duty to monitor" "or ignored obvious signs of fraud").

Second, Defendants attempt to disparage Thornton-Trump by noting that he made his Presentation shortly after joining the Company. Mot. at 17. But Thornton-Trump is an expert in cybersecurity. ¶64. Before making his Presentation, he conducted extensive research into SolarWinds' security practices, including asking colleagues for any documentation regarding cybersecurity and speaking to people outside the Company about active attacks in the cybersecurity space. ¶¶67, 73. That he was able to identify the deficiencies in SolarWinds'

cybersecurity in such a short amount of time, if anything, demonstrates just how obvious and egregious the deficiencies were. *See In re New Century*, 588 F. Supp. 2d 1206, 1231 (C.D. Cal. 2008) ("[T]he fact that the new CEO … discovered the accounting violations within months of taking the position is a strong indication that these accounting violations were obvious enough that a new officer found them quickly."); *see also In re Reliance Sec. Litig.*, 91 F. Supp. 2d 706, 725 (D. Del. 2000) (allegations that new CFO "discovered that the Company's income was overstated within weeks of becoming its CFO" support scienter).[4]

Third, Defendants ask the Court to assume (because they say so) that SolarWinds made dramatic reforms between the date of Mr. Thornton-Trump's resignation and the start of the Class Period. But it is Lead Plaintiff—not Defendants—that is entitled to reasonable inferences at this stage. And it is reasonable to infer that SolarWinds did ***not*** reform after Mr. Thornton-Trump's Presentation. Ten SolarWinds employees have provided consistent accounts that unquestionably confirm that the Company did ***not*** adopt any of the lacking cybersecurity controls after his departure. *See* ¶¶113-49. Investigative journalists likewise found that the deficiencies identified by Mr. Thornton-Trump persisted, unabated until the cyberbreach at the end of the Class Period. *See* ¶¶113, 147. And, finally, it is beyond dispute that the password for the Company's Update Server—i.e., the keys to the source of the data breach—were publicly available and compromised

[4] Defendants' cases are distinguishable. In *Shah v. GenVec, Inc.*, a former employee's allegations were discounted because he provided statements that were "at odds with every other account in the complaint and the documentary evidence." 2013 WL 5348133, at *5 n.7 (D. Md. Sept. 20, 2013). Mr. Thornton-Trump's account, on the other hand, is ***corroborated*** by each of the 10 other former SolarWinds employees in the Complaint. In *Zucco Partners, LLC v. Digimarc Corp.*, the former employees in question had "only secondhand information" of the relevant workings of the relevant company departments, whereas Mr. Thornton-Trump was the Company's Global Cybersecurity Strategist and commented on the conditions he personally observed. *See* 552 F.3d 981, 996 (9th Cir. 2009), *as amended* (Feb. 10, 2009).

for years. *See* ¶¶105-09. Under these circumstances, Lead Plaintiff is entitled to the "reasonable inference that no changes had been made in the interim." *BofI*, 2017 WL 2257980, at *11, *13.

Defendants gain nothing by noting that Thornton-Trump stated in his Presentation that SolarWinds ***could*** make "significant progress and achievement" within a year. Mot. at 17 n.15. That SolarWinds ***could have*** made progress in a year does not mean that it ***did***. And Lead Plaintiff's allegations make clear that SolarWinds did not make any progress.[5]

Finally, Defendants try to minimize Thornton-Trump's Presentation by asserting that he did not "identify any facts contradicting or conflicting with the challenged statements." Mot. at 19. This is factually wrong. For example, the Security Statement stated that SolarWinds had a dedicated "cybersecurity team," with "defined" "security roles and responsibilities." In truth, SolarWinds lacked any such security team—a specific failure that Thornton-Trump identified during his Presentation. *Compare* ¶75 *with* ¶43. As another example, the Security Statement stated that SolarWinds "provided [employees] with security training as part of new hire orientation." But Thornton-Trump told his colleagues during the meeting that the Company did not conduct cybersecurity training. *Compare* ¶78 *with* ¶¶47-48. Thornton-Trump's Presentation was clear as day: SolarWinds' "infrastructure and corporate systems exist in a precarious state." ¶¶77, 181. That he did not itemize each and every absent cybersecurity control is irrelevant—Defendants were on notice that SolarWinds was not secure. His Presentation strengthens the inference that SolarWinds and Defendant Thompson knew or were, at minimum, severely reckless

[5] Defendants further misstate the record by suggesting that Mr. Thornton-Trump's Presentation merely acknowledged the risk of cyberattack rather than identified cybersecurity deficiencies within the Company. Mot. at 19 & n.18. The Presentation went well beyond that. Among other things, the Presentation specifically stated that SolarWinds' "infrastructure and corporate systems exist in a precarious state" (¶77), with "No centralized reporting," "No centralized management," and "Silos of communication." (¶75).

in not finding out that the Company lacked the core cybersecurity controls that it represented having in the Security Statement.

b. By Refusing To Make The Necessary Cybersecurity Investments, Thompson And SolarWinds Were Able To Meet Analyst Earnings Estimates

The scienter inference is further strengthened by the fact that Defendant Thompson and SolarWinds' refusal to put in place the cybersecurity controls represented in the Security Statement enabled the Company to meet (barely) analyst consensus estimates during the Class Period—in some quarters, by as little as 1% of net income. SolarWinds recently announced that its cybersecurity reforms will cost the company $20 million to $25 million each year. ¶¶178, 190. The Complaint details how SolarWinds would have missed analyst earnings estimates throughout the Class Period had it spent this necessary amount to institute sufficient cybersecurity practices and controls. ¶190.

These facts further strengthen the scienter inference. *See In re Akorn, Inc. Sec. Litig.*, 240 F. Supp. 3d 802, 820 (N.D. Ill. 2017) ("Importantly, those violations made the difference between failure and success in meeting … Wall Street consensus revenue estimates for two quarters."); *In re AFC Enters., Inc. Sec. Litig.*, 348 F. Supp. 2d 1363, 1375 (N.D. Ga. 2004) ("precise meeting of analysts' estimates," among other facts, "are sufficient in totality to satisfy the pleading standard of the Reform Act").[6]

In response, Defendant Thompson asserts that his desire to prioritize short-term profits over long-term cybersecurity is "incoherent and runs counter to a common-sense understanding of

[6] Defendants erroneously attempt to liken these allegations to the "generalized motive allegations" that business executives always pursue growth and business opportunity. But unlike the cases cited by Defendants (*Eizenga*, *Tuchman* and *Shaw*), Defendant Thompson's motive was not simply to grow the business or create better business opportunities; it was to forego a particular expense—a sum certain—that would otherwise cause the Company to miss analyst estimates.

Thompson's interests." Thompson Mot. at 17. To be sure, Thompson's short-sighted decision to pursue short-term profits, meet analyst quarterly estimates, and focus on his receipt of outsized executive compensation awards, was the wrong decision for SolarWinds' long-term shareholders. But there is nothing "incoherent" in the notion that Thompson and the Private Equity Firms that controlled SolarWinds were motivated to take a short-term gamble: forego the cost of cybersecurity to derive personal profit, while betting that the risk of a cyberbreach will not materialize. *See Makor Issues & Rights, Ltd. v. Tellabs Inc.*, 513 F.3d 702, 710 (7th Cir. 2008) ("The fact that a gamble—concealing bad news in the hope that it will be overtaken by good news—fails is not inconsistent with its having been a considered, though because of the risk a reckless, gamble."); *Skiadas v. Acer Therapeutics Inc.*, 2020 WL 4208442, at *8 (S.D.N.Y. July 21, 2020) ("Skiadas alleges that Defendants gambled and lost. Skiadas is not arguing—no matter how many times Defendants say the opposite—that Defendants knew that the FDA would not approve EDSIVO.").

c. Defendant Thompson's Suspicious Class-Period Stock Sales Are Indicative Of Scienter

Defendant Thompson's outsized and presciently timed stock sales further bolster the scienter inference. During the Class Period, Defendant Thompson sold 39.16% of his SolarWinds shares. ¶192. This amounted to one million total shares, and his sales earned him more than $20 million. *Id.* The sales were suspicious in both their size and timing, with the bulk of the sales occurring during the short window between the time when SolarWinds was told by Palo Alto of a cyberbreach and the public announcement of the cyberbreach. ¶¶192-95; *see also Berger v. Compaq Comput. Corp.*, 1999 WL 33620108, at *17 (S.D. Tex. Dec. 22, 1999) ("Twenty percent

of a corporate insider's shares, especially where the dollar amounts are high, may constitute a 'suspicious amount' sufficient to support a scienter allegation.").[7]

The Complaint details why Defendant Thompson's Class Period insider stock sales were suspicious. *See* ¶¶192-95. In accordance with Fifth Circuit precedent, it compares Defendant Thompson's insider trades during the 26-month Class Period with trades during an equal amount of time prior to the Class Period (the "Control Period"). ¶193. This comparison shows that Defendant Thompson's sales during the Class Period were ***three times*** larger than his sales during the Control Period. *Id*. Even more, when Defendant Thompson's option-related sales during the Control Period are excluded (as they should be for this analysis), his Class Period sales are approximately ***nineteen times*** larger than his Control Period sales. *Id*.[8]

Defendant Thompson's contention that his stock sales were "innocent" because they were made pursuant to a 10b5-1 trading plan fails as a matter of law. The "trading plan" he refers to was put in place in August 2019 (i.e., ***during*** the Class Period)—making it irrelevant for purposes of analyzing the suspicious nature of his trades. *See Cent. Laborers' Pension Fund v. Integrated Elec. Servs Inc.*, 497 F.3d 546, 554 (5th Cir. 2007) ("[T]he attempt to use the 10b5-1 Plan as a non-suspicious explanation is flawed because, *inter alia*, [defendant] entered into the Plan during

[7] Defendants' argument that Lead Plaintiff has not sufficiently pled the details of the Palo Alto warning that there had been a breach is wrong: that Defendant Thompson's insider stock sales took place in such close proximity to the company being warned of such a breach indicates that Thompson was aware of the warning, and sold his stock anticipating a fallout once the information would become public knowledge. *See Rougier*, 2019 WL 6111516, at *13(allegations that insider defendants sold stock "immediately after" false or misleading statement, but before corrective disclosures, found to be indicative of motive).

[8] All of Defendant Thompson's "option-related" sales concerned shares acquired through Defendant Thompson's exercise of options, sold the same day that he acquired them. In each instance, Defendant Thompson retained the same number of shares before exercising the option as after the option-related sale. Accordingly, excluding "option-related" sales from this calculation presents a more relevant comparison of Defendant Thompson's Control Period sales.

the Class Period."); *In re ArthroCare Corp. Sec. Litig.*, 726 F. Supp. 2d 696, 722 (W.D. Tex. 2010) ("[W]hether or not the stocks in this case were sold pursuant to a 10b5–1 trading plan is irrelevant at this stage in the proceedings, as the existence of such a plan is an affirmative defense, which requires evidence of the plan itself and of details such as the date the plan was entered into…."). Likewise, Defendant Thompson's self-serving contention that he merely wanted to sell his stock before he retired has been rejected by the Fifth Circuit. *See id.* at 553-54 (rejecting defendant's explanation that it is "not unusual for a corporate officer to sell his stock shortly before resigning" in finding that CFO's sales "contribute to an inference of scienter"); s*ee also Rubinstein v. Collins*, 20 F.3d 160, 170 n.38 (5th Cir. 1994) (rejecting defendants' explanation "that these sales were innocuous because they were made in response to tax considerations"). At most, Thompson's litany of proffered excuses for his stock sales raises fact issues that cannot be decided in Defendants' favor now.

Also without merit is Defendant Thompson's argument that Defendant Brown's lack of insider sales undermines the scienter allegations against Defendant Thompson. The Fifth Circuit and courts around the country have held that "[t]he fact that not every one of the defendants may have sold stock does not defeat an inference of scienter at this stage of the litigation." *In re APAC Teleservice, Inc. Sec. Litig.*, 1999 WL 1052004, at *7 (S.D.N.Y. Nov. 19, 1999) (citing *Rubinstein*, 20 F.3d at 169-70); *see also Southland*, 365 F.3d at 380 (CEO's sale of 40% of stock contributed to inference of scienter as to him even though other defendants' sales were not suspicious).

d. The Fact That SolarWinds' New CEO Immediately Identified The Deficiencies In Its Cybersecurity Further Strengthens The Scienter Inference

The scienter inference is also strengthened by the fact that SolarWinds' new CEO, Sudhakar Ramakrishna, was able to quickly identify SolarWinds' lack of basic cybersecurity controls within just a matter of months of his joining the Company. *See* ¶¶168-75. The Complaint

details how, shortly upon joining SolarWinds, Ramakrishna announced several cybersecurity initiatives to bring the Company in line with the Security Statement. These included establishing a dedicated security team, reviewing the Company's password management policies, enforcing limited access privilege policies, and beginning to segment its networks—i.e., controls that SolarWinds told investors it ***already*** had in place since the start of the Class Period. *See* ¶¶43, 52, 55, 171-76.

Defendants' argument that CEO Ramakrishna's admission of the post-Class Period reforms "say nothing" about Defendants' scienter during the Class Period is wrong. Scienter exists if a defendant acted with an "intent to deceive" ***or*** "severe recklessness" (*Spitzberg*, 758 F.3d at 684) and can be shown through direct ***or*** circumstantial evidence (*see Lormand*, 565 F.3d at 251). The fact that SolarWinds' new CEO identified the deficiencies in SolarWinds' cybersecurity and expeditiously remedied these deficiencies within a matter of months strengthens the scienter inference. *See Plotkin*, 407 F.3d at 698 ("[A]llegations of later-emerging facts can … provide warrant for inferences about an earlier situation."); *see also In re Resideo Techs., Inc., Sec. Litig.*, 2021 WL 1195740, at *6 (D. Minn. Mar. 30, 2021) (the "rapid discovery of undisclosed problems by the new chief financial officer" supported scienter); *New Century*, 588 F. Supp. 2d at 1231 ("[T]he fact that the new CEO … discovered the accounting violations within months of taking the position is a strong indication that these accounting violations were obvious enough that a new officer found them quickly.").

3. Defendants' Competing Inference Is Not More Compelling

To defeat Lead Plaintiff's scienter inference, Defendants bear the heavy burden of offering a more compelling inference. The Fifth Circuit has emphasized that "a plaintiff … must only 'plead facts rendering an inference of scienter at least as likely as any plausible opposing inference'" and "a tie favors the plaintiff." *Lormand*, 565 F.3d at 250. In considering scienter

allegations at the pleading stage, "[t]he inquiry is whether all of the facts alleged, taken collectively, give rise to a strong plausible inference of scienter." *Id.* at 251. Because the Court "must … accept all factual allegations in the complaint as true," *see id.* at 232, "Defendants cannot introduce disputed facts through judicial notice at the dismissal stage in a motion to dismiss." *Miller v. Stroman*, 2020 WL 2494576, at *3 (W.D. Tex. May 14, 2020).

Defendants improperly attempt to construct a competing narrative through self-serving statements and disputed "facts" drawn from exhibits that cannot be credited for their truth at this stage. Their "competing inference" turns on their assertion (Mot. at 31) that they "were responsible stewards of a growing business operating in an industry distinctly susceptible to the risk of sophisticated cyber espionage." But would "responsible stewards" of a software company, whose largest customers were government agencies responsible for national security, lack the most fundamental cybersecurity controls set forth in their security statement? Would "responsible stewards" attempt to lure customers to buy their products by emphasizing the importance of cybersecurity, but then not actually put in place cybersecurity controls? Would "responsible stewards" allow an intern to set the quintessential weak password to unlock the company's critical Update Server and permit the password to remain unchanged for two years? Would "responsible stewards" receive Thornton-Trump's dire warnings and do nothing, until a new CEO enters the Company three years later and insists upon change? As the Fifth Circuit has held, "an egregious refusal to see the obvious, or to investigate the doubtful, may … give rise to an inference of recklessness." *Plotkin*, 407 F.3d at 700 (citing *Novak*, 216 F.3d at 308). The obvious reality of the Executive Defendants' "stewardship" of SolarWinds is far removed from the doubtful, rosy picture Defendants attempt to paint. Scienter is the far more compelling inference here.

C. The Complaint Adequately Pleads Loss Causation

Loss causation is the "causal connection between the material misrepresentation and the loss" suffered by Plaintiffs and the putative class. *Dura Pharms., Inc. v. Broudo*, 544 U.S. 336, 342 (2005). In this Circuit, loss causation allegations are subject to Rule 8's liberal pleading standards and must merely "provide a defendant with some indication of the loss and the causal connection that the plaintiff has in mind." *Pub. Emps. Ret. Sys. of Miss., P.R. Tchrs. Ret. Sys. v. Amedisys, Inc.*, 769 F.3d 313, 321 (5th Cir. 2014). Lead Plaintiff need only "allege enough facts to give rise to a reasonable hope or expectation that discovery will reveal a 'facially plausible causal relationship between the alleged fraudulent statements or omissions and [P]laintiff's economic loss, followed by the leaking out of relevant or related truth about the fraud that caused a significant part of the depreciation of the stock ….'" *In re TETRA Techs., Inc. Sec. Litig.*, 2009 WL 6325540, at *9 (S.D. Tex. July 9, 2009) (quoting *Lormand*, 565 F.3d at 258). Lead Plaintiff has readily satisfied the pleading standard here.

The Complaint details how SolarWinds' seriously deficient cybersecurity framework proximately caused the breach, and the revelations of both the breach and the security deficiencies proximately caused SolarWinds' stock price to drop. *See* ¶¶150, 152, 154, 156-163. Specifically, the Complaint alleges that the hackers uploaded infected update files on the SolarWinds Update Server for download by customers. ¶151. Every time a customer downloaded such a file, the hackers gained unfettered access to that customer's data. *Id.* The hackers took advantage of SolarWinds' glaring security deficiencies to infiltrate the Company's update files and remain undetected for over a year. ¶152. The Company's un-secure platform enabled and attracted the hackers—making the Company an "easy target," as cybersecurity experts have explained. ¶¶153-54.

The Complaint alleges that investors learned the truth through a series of disclosures: (i) on December 13-14, 2020, investors learned about the breach and the possibility that 18,000 customers were impacted (¶¶225-27); (ii) on December 15, 2020, investors learned that the "solarwinds123" password had been publicly available for a year-and-a-half and the malware that caused the breach remained available for download days after Defendants learned of the breach (¶¶229-30); and (iii) on December 17, 2020, investors learned that even more customers had been impacted, and that the NSA and the Department of Energy had been compromised (¶232). On these dates, SolarWinds stock price fell 17%, 8%, and 19%, respectively. ¶¶227, 231, 233. These allegations are more than sufficient to meet the liberal Rule 8(a) pleading requirement for proximate cause. *See, e.g.*, *Amedisys*, 769 F.3d at 326 (finding that loss causation is properly pled where the complaint "sets forth specific allegations of a series of partial corrective disclosures, joined with the subsequent fall in [the company's] stock value"); *Cobalt*, 2016 WL 215476, at *6 (finding that allegations of stock price declines of 21%, 11%, and 11.5% after partial disclosures were sufficient to show loss causation).

Lead Plaintiff has alleged a direct link between the cyberbreach and the absence of cybersecurity controls at SolarWinds. *See* ¶¶150, 152, 154, 156-163. Determining whether Lead Plaintiff's or Defendants' account of the cyberbreach is correct is an intensely factual inquiry inappropriate for determination at the pleadings stage, particularly when judged (as it must be) under the Rule 8 standard. *See Aubrey v. Barlin*, 2010 WL 3909332, at *12 (W.D. Tex. Sept. 29, 2010) ("Lahr's arguments to the contrary are factual disputes over the 'actual' cause of the losses; thus, they are not appropriate in the context of a motion to dismiss, in which we must take all of Plaintiff's well-pleaded facts as true.").

Defendants also argue that the December 13-17, 2020 revelations are not corrective disclosures. Mot. at 38-40. But Defendants misapprehend the "loss causation" test. In the Fifth Circuit, a plaintiff must merely "allege the truth that emerged was 'related to' or 'relevant to' the defendants' fraud and earlier misstatements." *Amedisys*, 769 F.3d at 321. "The test for relevant truth simply means that the truth disclosed must make the existence of the actionable fraud more probable than it would be without that alleged fact, taken as true." *Id.* Because the truth about Defendants' security practices and the breach are clearly related and relevant to Defendants' misstatements, Lead Plaintiff has met its burden here. *Id*.

The court's decision in *Equifax* also concerned a devastating data breach and similar loss causation contentions. 357 F. Supp. 3d 1189. There, the plaintiffs alleged that Equifax made false statements concerning its cybersecurity systems and compliance with data protection laws. Like Defendants here, Equifax argued "that the announcements to the public of the Data Breach … did not 'reveal' that the prior statements concerning Equifax's data security were false, and thus were not a corrective disclosure." *Id.* at 1249. In rejecting this argument, the court explained that "a disclosure need not precisely mirror an earlier misrepresentation, but instead must relate to the misrepresentation and not other negative information about the company." *Id.* The court found that the totality of the disclosures "combined to disclose the truth to investors"—as is the case here. *Id.* at 1250.

In *In re BP p.l.c. Securities Litigation*, the court also considered similar allegations: that "the explosion aboard the Deepwater Horizon, and the resulting uncontrolled oil spill, were the means through which the market learned that Defendants' public relations campaign on process safety had been nothing more than empty rhetoric." 922 F. Supp. 2d 600, 638 (S.D. Tex. 2013). In rejecting defendants' challenge to loss causation, the *BP* court explained that a corrective

disclosure need not "consist of a fact-by-fact recounting of the alleged fraud," but rather "simply has to unwind, slowly or all at once, the inaccurate depiction of the company's affairs as presented in the preceding allegedly fraudulent or misleading statements." *Id.* Just as in *BP*, the SolarWinds cyberbreach was one of the "means through which the market learned that Defendants' public relations campaign on [cybersecurity] had been nothing more than empty rhetoric." *Id.* And the revelations about the cyberbreach, along with further disclosures about SolarWinds' lack of cybersecurity controls, unwound the inaccurate depiction set forth by Defendants' false and misleading statements. The Rule 8 pleading requirement for loss causation is plainly satisfied in this case.

D. The Complaint Adequately Pleads Control Person Claims

The Complaint's allegations also amply meet the standard for stating a Section 20(a) control person claim against the Private Equity Firms. "A prima facie case of Section 20(a) claims are subject to the pleading requirements of Federal Rule of Civil Procedure 8, not the heightened requirements of Rule 9(b); therefore, only a statement giving [the defendant] fair notice of the plaintiff's claim and the basis of the allegation is required." *Zix Corp.*, 2006 WL 2739352, at *9. Significantly, "[a]t the pleading stage, a plaintiff need only allege that the defendant possessed the power to control the primary violator, not that control was exercised." *Camelot Event Driven Fund v. Alta Mesa Res., Inc.*, 2021 WL 1416025, at *10 (S.D. Tex. Apr. 14, 2021). Moreover, Section 20(a) "has been read liberally and its provisions were enacted to expand, rather than restrict the scope of liability under the securities laws." *McNamara v. Bre-X Mins., Ltd.*, 46 F. Supp. 2d 628, 635 (E.D. Tex. 1999).

To state a control-person claim under Section 20(a), a plaintiff need only allege "(1) a primary violation by a controlled person; and (2) direct or indirect control of the primary violator by the defendant." *One Longhorn Land I, L.P. v. Defendant FF Arabian, LLC*, 2015 WL 7432360,

at *2 (E.D. Tex. Nov. 23, 2015). Lead Plaintiff has stated a primary violation under Section 10(b) against SolarWinds, as discussed above. *See supra* at §§IIIA-C. Accordingly, Lead Plaintiff need only plausibly allege under Rule 8(a) that the Controlling Entity Defendants had "direct or indirect control" over SolarWinds. Lead Plaintiff has met the pleading requirements.

First, throughout the Class Period, the Controlling Entity Defendants were the largest SolarWinds stockholders and had the right to appoint a majority of the Company's directors to the Board of Directors. Specifically, at the start of the Class Period, each of the Controlling Entity Defendants owned over 40% of the Company's stock. ¶¶19-20. Although both firms sold stock during the Class Period to net nearly $730 million in total profit, they jointly remained the majority shareholders throughout the Class Period. *Id.* Furthermore, seven of the board's ten members were partners, principals, or directors of the Controlling Entity Defendants. ¶¶19-20, 266-67. Those board members were entitled to constitute majorities of all committees other than the audit committee. ¶266. Their stock ownership and board control allowed them to control the Company's day-to-day operations to their own ends. ¶¶28, 263. In this Circuit, the "term 'control' … means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract, or otherwise." *G.A. Thompson & Co. v. Partridge*, 636 F.2d 945, 957-58 (5th Cir. 1981) (quoting 17 C.F.R. § 230.405(f) (1979)). The Controlling Entity Defendants had the power to control.

Second, SolarWinds admitted that the Private Equity Firms were control persons. In its SEC filings during the Class Period, SolarWinds repeatedly described itself as a "controlled company." ¶265. SolarWinds admitted that the Private Equity Firms "could exert ***significant influence*** over [SolarWinds'] operations and business strategy and would ***together have sufficient***

voting power to effectively control the outcome of matters requiring stockholder approval." *Id.* SolarWinds further acknowledged that, because of the Controlling Entity Defendants' "concentration of ownership" of SolarWinds stock, they could unilaterally "***delay or prevent*** proxy contests, mergers, tender offers, open-market purchase programs or other purchases of [SolarWinds] common stock that might otherwise give [investors] the opportunity to realize a premium over the then-prevailing market price of [SolarWinds] common stock." ¶266. Such admissions by SolarWinds itself are indicative of the Private Equity Firms' power to exert control over the Company. *See Cobalt*, 2016 WL 215476, at *11 (noting that, in its SEC filings, "Cobalt identified itself as a 'controlled company'" and disclosed that the controlling entities "'have significant influence'" over Cobalt in sustaining control person liability claims); *City of Omaha Police & Fire Ret. Sys. v. Evoqua Water Tech. Corp.*, 450 F. Supp. 3d 379, 428 (S.D.N.Y. 2020) (noting that Evoqua's SEC filings acknowledged its status as a "controlled company" and the majority-stockholder controlling defendants' ability to "influence all major corporate decisions").

Defendants cite *In re Kosmos Energy Ltd. Securities Litigation*, 955 F. Supp. 2d 658 (N.D. Tex. 2013), in support of their contention that a company's election to be treated as a "controlled entity" under the New York Stock Exchange rules is "irrelevant" to the question of control person liability. Silver Lake Mot. at 8; Thoma Bravo Mot. at 14-15. But Lead Plaintiff has not relied on SolarWinds' mere "election" to be "treated as" a controlled company per the NYSE rules. Additionally, unlike in *Kosmos*, SolarWinds admitted ***why*** and ***how*** it was a controlled company, including that the Private Equity Firms "could exert ***significant influence*** over [SolarWinds'] operations and business strategy and would ***together have sufficient voting power to effectively control*** the outcome of matters requiring stockholder approval." ¶265.

Third, the Controlling Entity Defendants acted together to amass and retain control over SolarWinds. As alleged in the Complaint, the Private Equity Firms acted in unison, buying and taking the Company private ***together*** in 2016—each paying $1.3 billion for their respective halves—and then taking the Company public ***together*** again in 2018, retaining ***equal amounts*** of shares of the Company. ¶¶14, 27. Plus, when either Private Equity Firm sold their SolarWinds shares after the 2018 IPO, they did so together, on the same day, and in nearly identical amounts. ¶¶19-20, 194. Where, as here, Lead Plaintiff alleges that the Controlling Entity Defendants acted in concert and had the combined power to control SolarWinds, Lead Plaintiff has successfully alleged control person liability against them. *See Cobalt*, 2016 WL 215476, at *11 (crediting allegations that five private equity firms "*together* controlled Cobalt based … on their significant stock ownership and ability to elect a majority of Cobalt's Board of Directors"); *Evoqua Water*, 450 F. Supp. 3d at 427 (finding that eleven private equity entities acted together to have joint control of the company).

In any event, a control person claim can be adequately alleged even without an individual defendant having majority shareholder status. *See Hill York Corp. v. Am. Int'l Franchises, Inc.*, 448 F.2d 680, 694 (5th Cir. 1971). Such "formalism alone is not determinative of the question since the statute refers to control by stock ownership, agency *or otherwise*." *Id.* "While a majority shareholder might as a matter of law be held to 'control' the entity regardless of his actual participation in management decisions and the specific transaction in question, the absence of a substantial ownership of shares does not foreclose liability under the Act as a controlling person." *Id.* at 694 n.20.

To be sure, Lead Plaintiff does not, as Defendant Silver Lake incorrectly suggests (Silver Lake Mot. at 6-7), need to allege the actual ***exercise*** of control to state a Section 20(a) claim. "At

this stage, a plaintiff need only allege that "[the controlling entity] possessed the power to control the primary violator, not that control was exercised." *One Longhorn Land*, 2015 WL 7432360, at *3. Nor must Lead Plaintiff allege that the Controlling Entity Defendants participated in the underlying Exchange Act violation. *Id.* at *2.[9] Rather, the "power to control" is the relevant inquiry, and the Complaint amply alleges the Controlling Entity Defendants' power to control SolarWinds.

Defendant Silver Lake argues that it has not been put on notice of the claims against it because "the Complaint indiscriminately lumps together *various sets* of Defendants." Silver Lake Mot. at 4. This is a reference to the fact that (i) Lead Plaintiff named both Silver Lake Group L.L.C. ("SLG") and Silver Lake Technology Management, L.L.C. ("SLTM") as defendants, and (ii) that the Complaint oftentimes refers to the actions and control of both Defendants Silver Lake and Thoma Bravo in the aggregate. *Id.* at 4-6; *see also* Thoma Bravo Mot. at 8 n.4. But Defendants themselves admit that "three funds managed by SLTM ***collectively*** owned approximately 40% of SolarWinds' outstanding stock during the class period," and argue no independent basis as to why SLG should be dismissed from this action. *See* Silver Lake Mot. at 1-2. It is undisputed that SLTM controls Silver Lake's share of the majority interest in SolarWinds at the heart of these allegations. And, as to the references to the allegations of the Private Equity Firms in the aggregate, as stated above, the Private Equity Firms acted ***together*** since first taking the Company private in 2016 and public in 2018. *See supra* at 70.

[9] Defendant Thoma Bravo misleadingly states that "Congress did not intend for plaintiffs to sweep in investors who did not direct or participate in the alleged primary violation." (Thoma Bravo Mot. at 5). The law is clear that control person liability does ***not*** require a showing of either "direction" of or "participation" in the violation. *One Longhorn Land*, 2015 WL 7432360, at *2; *Cobalt*, 2016 WL 215476, at *11.

The Controlling Entity Defendants also cite to *Zishka* in support of their contention that Lead Plaintiff has not alleged that the Controlling Entity Defendants had "day-to-day" control over the Company. *See* Silver Lake Mot. at 6-7; *Zishka v. Am. Pad & Paper Co.*, 2001 WL 1748741, at *1 (N.D. Tex. Sept. 28, 2001). However, the Fifth Circuit "has not yet decided whether a plaintiff must show that the alleged controlling person had 'effective day-to-day control.'" *Heck v. Triche*, 775 F.3d 265, 283 n.18 (5th Cir. 2014). The Court should not impose such a stringent requirement, especially considering the liberal Rule 8 pleading requirement that applies to control person claims. *See Bre-X Mins.*, 46 F. Supp. 2d at 635. And, in any event, Lead Plaintiff has alleged facts that amount to "effective day-to-day control."

Moreover, Lead Plaintiff alleges much more than the Private Equity Firms' "status alone" as major shareholders in support of their control person claim. *See* Silver Lake Mot. at 6-7; Thoma Bravo Mot. at 5, 14-15. In addition to being major shareholders collectively owning approximately 80% of all shares, the Controlling Entity Defendants occupied the majority of the seats on the Company's Board of Directors and its committees. As acknowledged in SolarWinds' SEC filings, they also had the power to influence any major corporate decision without any threat of a proxy contest from dissenting minority shareholders. *See Cobalt*, 2016 WL 215476, at *11 (noting the plaintiffs' allegations that the private equity firms held a majority of the stock of Cobalt and a majority of the seats on the board and its committees, as well as SEC filing statements concerning the firms' ability to influence Cobalt's business decisions).

Finally, Defendants' challenges raise, at most, a hotly contested factual dispute about the level of control exercised by the Controlling Entity Defendants. Such fact disputes are not appropriate for resolution on the pleadings. *See In re Refco, Inc. Sec. Litig.*, 503 F. Supp. 2d 611,

638-40 (S.D.N.Y. 2007) (sustaining control person claims and noting that "it was not implausible that plaintiffs could develop a record that could support a finding of control").

IV. CONCLUSION

For these reasons, Defendants' Motions should be denied. In the event that the Court dismisses this action, Lead Plaintiff respectfully requests leave to amend.

DATED: October 1, 2021

MARTIN & DROUGHT, P.C.

/s/ Gerald T. Drought
Gerald T. Drought
State Bar No. 06134800
Federal Bar No. 8942
Frank B. Burney
State Bar No. 03438100
Weston Centre
112 E. Pecan Street, Suite 1616
San Antonio, Texas 78205
Tel: (210) 227-7591
Fax: (210) 227-7924
gdrought@mdtlaw.com

Liaison Counsel for Lead Plaintiff New York City District Council of Carpenters Pension Fund

BERNSTEIN LITOWITZ BERGER & GROSSMANN LLP
John J. Rizio-Hamilton (admitted *pro hac vice*)
Jonathan D. Uslaner (admitted *pro hac vice*)
Benjamin W. Horowitz (admitted *pro hac vice*)
Thomas Z. Sperber (admitted *pro hac vice*)
1251 Avenue of the Americas
New York, New York 10020
Telephone: (212) 554-1400
Facsimile: (212) 554-1444
Johnr@blbglaw.com
JonathanU@blbglaw.com
Will.Horowitz@blbglaw.com
Thomas.Sperber@blbglaw.com

Lead Counsel for Lead Plaintiff New York City District Council of Carpenters Pension Fund and the Class

CERTIFICATE OF SERVICE

I hereby certify that on October 1, 2021, all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF Filing system.

/s/ Gerald T. Drought
GERALD T. DROUGHT